Políticas y normas de seguridad de sistemas informáticos

Autor: Josué Daniel García Samperio

Tesina presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarras

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

" POLÍTICAS Y NORMAS DE SEGURIDAD DE SISTEMAS INFORMÁTICOS "

TESINA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:

Josue Daniel García Samperio

No. DE ACUERDO 952006 CLAVE 16PSU0014Q

ASESOR DE TESINA:

M.A. Ing. Sergio Francisco Barraza Ibarra

MORELIA, MICHOACÁN, MÉXICO. MAYO 2004.

Dedicatorias

A dios por haberme permitido realizar esta meta de mi vida y siempre estar a mi lado para guiarme.

A mis padres, Salvador y Lina por el apoyo y confianza que siempre me han brindado para seguir adelante. Gracias por llenar mi vida con tanta felicidad.

A mi hermana Sendy y a Oscar por sus consejos y ánimos positivos que siempre me expresan.

A toda mi FAMILIA por las palabras de aliento para lograr mis metas y en especial a mi tío Lico Samperio por su amistad de amigos y sus consejos que me sirvieron para concluir con esta etapa.

A mi asesor Ing. Sergio Francisco Barraza por compartir su experiencia y conocimientos para la realización de esta tesina y de toda la licenciatura.

Para todos los que me han demostrado una amistad sincera y honesta en especial para Jessica, Hassel, Rafael, Moisés, Abrahán, Jorge, Ulises, Venancio, Felipe, Omar, Mauricio, Cesar, frank.
Los buenos amigos son difíciles de encontrar mas difíciles de dejar e imposibles de olvidar.

INDICE GENERAL

INTRODUCCIÓN **4**
II JUSTIFICACIÓN **6**
2.1 Objetivo general 6
2.2 Objetivos particulares 6
III SISTEMA OPERATIVO **7**
3 Necesidad de Sistema Operativo 7
3.1 Vista histórica 7
3.2 Definición. 8
3.3 Tipos de gestión de procesos de un Sistema Operativo. 8
3.3.1 Sistemas por lotes. 9
3.3.2 Multiprogramación. 9
3.3.3 Sistemas distribuidos. 10
3.4 Arquitectura de un Sistema Operativo 11
3.5 Diferentes funciones de un Sistemas operativos. 12
3.6 Tipos de llamadas al sistema, o servicios que ofrece el sistema. 13
3.7 Reseña histórica. 14
IV WINDOWS **15**
4 Historia de Windows. 15
4.1 Windows 1.0 15
4.2 Microsoft Windows 2.0 15
4.3 Windows 3.0 16
4.4 OS/2 1 16
4.5 Windows 3.1 y Windows 3.11 17
4.6 Windows NT 17
4.7 Windows 95 18
4.8 Windows NT 3.1 18
4.9 Windows 95 19
4.10 Windows NT 4.0 19
4.11 Windows 98 19
4.12 Windows 98 Second Edition 20
4.13 Windows Millennium Edition 20
4.14 Windows 2000 20
4.15 Windows XP 20
4.16 Windows CE 21
V TÉCNICAS DE PROTECCIÓN **22**
5.1 Control de accesos por computadora. 22
5.1.1 Identificadores. 22
5.1.2 Filtros por dirección MAC. 23
5.1.3 Filtrado por nombre o dirección de red y puerto. 25
5.1.4 Filtros con Routers o Firewalls 26
5.1.5 Ataques al control por IP o nombre. 27
5.2 Control de acceso de usuario. 28

5.2.1 Características generales 28
5.2.2 Control por contraseñas. 30
5.2.3 Ataques a contraseñas 31
5.2.4 Defensas a ataques a contraseñas. 33
5.2.5 Sistemas biométricos. 35
5.2.6 Acceso con objetos físicos: Tokens. 38
5.2.7 Acceso con certificados digitales 39
VI CRIPTOGRAFÍA 43
5 Introducción. 43
6.1 Ramas de la criptografía. 43
6.2 Problemas de seguridad que resuelve la criptografía. 44
VII CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA 46
7.1 Criptografía Simétrica. 46
7.1.2 DES 47
7.1.2 Funciones Hash. 48
7.2 Criptografía Asimétrica. 49
7.2.1 RSA. 50
7.2.2 CCE 51
VIII SOFTWARE DE CONTROL 52
8.1 Autenticación kerberos. 52
8.1.1 Introducción. 52
8.1.2 Características. 52
8.1.3 Funcionamiento. 53
8.1.4 Autenticación de usuario. 54
8.1.5 Autenticación de servicios. 55
8.1.6 Instalación de Kerberos. 56
8.2 Autenticación Windows NT. 57
8.2.1 Esquema general. 57
8.2.2 Modelo de trajo en grupo. 58
8.2.3 Modelo de dominios. 60
8.2.4 Relaciones de confianza entre dominios. 61
8.2.5 Diferencias conceptuales con otros sistemas centralizados 62
IX POLÍTICAS DE SEGURIDAD EN RED 64
9.1 Desarrollo de políticas de seguridad 64
9.2 Aspectos a considerar para una política de seguridad. 64
9.3 Estrategias de seguridad. 65
9.3.1 Política global de seguridad 65
9.3.2 Análisis de riesgos. 66
9.3.3 Medidas de seguridad. 66
X AUDITORIA INFORMÁTICA 67
10 Estructura de los estándares para la práctica profesional de la auditoria de sistemas de información 67
10.1 Introducción a las Normas Generales para Auditoria de Sistemas de Información. 67
10.2 Necesidad de Normas de Auditoria de Sistemas de Información. 67
10.3 Definición de la Auditoria de Sistemas de Información 68

10.4 Objetivos..... 68
10.5 Alcance y Autoridad de las Normas de Auditoria de Sistemas de Información. 69
10.6 Relación entre las Normas de Auditoria de Sistemas de Información y otras Normas de Auditoria. 70
10.7 Código de ética profesional. 70
10.8 Normas generales de auditoria de información. 71
XI MARCO JURÍDICO DE PROTECCIÓN DE DATOS 75
11.1 Introducción. 75
11.2 Delitos Informáticos. 75
11.2.1 Ámbito federal. 75
11.2.2 Ámbito local. 75
11.3 Contratos Electrónicos. 76
11.4 Protección de la privacidad y de la información. 76
11.5 Propiedad Intelectual. 76
11.6 Computo Forense. 76
11.7 Contenidos de Internet. 77
11.8 Código Penal Federal. 77
11.8.1 Capitulo I 77
11.8.2 Capitulo II 78
XII ANEXO I 80
12 20 Consejos para el usuario de plataformas Windows. 80
12.1 10 Básicas para la Seguridad de tu plataforma Windows como usuario conectado a Internet. 80
12.2 10 Básicas para la Seguridad de la Información en su Sistema como usuario conectado a Internet. 81
XIII CONCLUSIONES 83
XIV BIBLIOGRAFÍA 84

Introducción

Reconozcámoslo sin complejos: El mayor agujero de seguridad no se encuentra en ningún producto de Microsoft.

La vulnerabilidad más grave está localizada en el cerebro de la persona que se sienta delante de la pantalla y desplaza el puntero del ratón con su mano.

Y es que, si lo pensamos con detenimiento, no deja de resultar increíble que se sigan produciendo, cada cierto tiempo, epidemias masivas de virus, troyanos y gusanos a través del correo electrónico.

Todos estos intrusos necesitan que sea el usuario quien abra el archivo adjunto en el mensaje recibido, y es aquí donde surge el flagrante delito.

El intruso no necesita idear nuevas y complicadas técnicas de infección, ni avanzados mecanismos de ocultación. Simplemente aprovechando esta actitud la llamada "Ingeniería Social" es posible convencer a cualquier usuario poco avezado para que haga exactamente lo que el intruso quiera; además, no estamos únicamente ante delitos contra la privacidad o integridad de nuestros datos (virus, gusanos y troyanos), sino también de una posible reducción de la productividad, sobre todo en entornos corporativos.

En definitiva, es el usuario, en último extremo, quien debe evaluar el alcance y las implicaciones de sus acciones. Es, sencillamente, nuestro trabajo y nuestra responsabilidad.

En resumen debemos de mencionar que no existe un sistema informático que garantice al 100% la seguridad de la información debido a la inmensa mayoría de formas diferentes con que se puede romper la seguridad de un sistema.

Sin embargo una buena planeación de la estrategia para dar seguridad a la información puede resultar desde la salvación de una empresa hasta la obtención de grandes ganancias directas en pesos, o como ganancias indirectas mejorando la imagen y la seguridad de la empresa.

Uno de los objetivos principales de establecer una política de seguridad es de reducir al mínimo los riegos posibles, implementando adecuadamente las diferentes medidas de seguridad.

II Justificación

El uso de técnicas de la informática forense tiene como propósito prevenir los principales agujeros de seguridad en un sistema informático. La seguridad en general debe de ser considerada como un aspecto de gran importancia en cualquier empresa que trabaje con sistemas informáticos. El hecho que gran parte de actividades humanas sea cada vez más dependiente de los sistemas informáticos hace que la seguridad juegue un papel importante.

2.1 Objetivo general

El propósito del presente trabajo es estructurar una metodología que permita a los administradores de redes, realizar un estudio para identificar y reparar los posibles agujeros de seguridad que puedan ser vulnerables a los sistemas informáticos.

2.2 Objetivos particulares

- ✓ Conocer los procedimientos de la informática forense para poder prevenir y corregir los agujeros de seguridad que se pueden presentar en un sistema informático.
- ✓ Crear conciencia y formación a los usuarios y administradores de redes sobre el buen manejo de los sistemas informáticos para protegerlos de cualquier ataque posible.
- ✓ Establecer estándares entre los administradores de redes en el desarrollo, implementación, mantenimiento y operación de políticas de seguridad.
- ✓ Mantener la confidencialidad y calidad de la información que se maneje en las empresas.

III Sistema Operativo

3 Necesidad de Sistema Operativo

3.1 Vista histórica

En un principio solo existía el hardware de la computadora. Las primeras computadoras eran (físicamente) grandes máquinas que se operaban desde una consola. El programador escribía un programa y luego lo controlaba directamente. En primer lugar, el programa se cargaba manualmente en la memoria, desde los interruptores del tablero frontal, desde una cinta de papel o desde tarjetas perforadas. Luego se pulsaban los botones adecuados para establecer la dirección de inicio y comenzar la ejecución del programa. Mientras este se ejecutaba, el programador-operador lo podía supervisar observando las luces en la consola. Si se descubrían errores, el programador podía detener el programa, examinar el contenido de la memoria y los registros y depurar el programa directamente desde la consola. La salida del programa se imprimía, o se perforaba en cintas de papel o tarjetas para su impresión posterior. Un aspecto importante de ese entorno era su naturaleza interactiva directa. El programador también era el operador del sistema informático.

Las computadoras, sobretodo los centrales de gran tamaño, han sido siempre máquinas muy costosas. Por ello, los dueños han deseado que estas máquinas efectúen la mayor cantidad posible de cálculos. Hoy en día, esta situación también se aplica a los microprocesadores de menor precio, de los cuales, a pesar de no ser tan costosos, siempre se espera que logren el mayor número posible de cálculos. El cambio a los sistemas por lotes con secuenciación automática de trabajos se efectuó para mejorar el rendimiento. El problema es que las personas somos demasiado lentas. Por lo tanto, es deseable sustituir la intervención humana por el software del sistema operativo. Aún con esta secuenciación automática de trabajos, la computadora todavía tiene periodos de inactividad. El problema es la velocidad de los dispositivos mecánicos de entrada y salida, los cuales son intrínsecamente más lentos que los

dispositivos electrónicos. Una computadora lenta trabaja en el orden de los microsegundos, pues ejecuta millones de instrucciones por segundo. La solución que se encontró a esto fue el uso de buffers o tapones que se anticipaban al programa leyendo los datos y dejándolos en memoria antes de que se originara la orden de leerlos, con lo que se acelera la ejecución total del programa.

3.2 Definición.

Concepto de Sistema Operativo: Es un programa que actúa como intermediario entre el usuario y el hardware de una computadora y su propósito es proporcionar un entorno en el cual el usuario pueda ejecutar programas.

Objetivo principal:

El objetivo principal de un sistema operativo es lograr que el sistema de computación se use de manera cómoda.

Objetivo secundario:

El objetivo secundario es que el hardware de la computadora se emplee de manera eficiente. Una definición más común es que el sistema operativo es el programa que se ejecuta todo el tiempo en la computadora, siendo programas de aplicación todos los demás.

3.3 Tipos de gestión de procesos de un Sistema Operativo.

En un principio, las computadoras se utilizaban desde la consola central. El software mejoró la comodidad de programar, pero necesitaba un tiempo considerable de preparación. Para reducir este tiempo, se contrataron operadores y los trabajos semejantes se agruparon en lotes. La computadora ya no tenía que esperar la intervención humana, aun así, la utilización de la computadora era muy lenta. Con el fin de mejorar el rendimiento global del sistema se

introdujo el concepto de multiprogramación, gracias al cual se almacenan en la memoria varios trabajos al mismo tiempo, lo que aumenta el rendimiento de la computadora y reduce el tiempo de ejecución de los trabajos.

3.3.1 Sistemas por lotes.

Cuando se desarrollaron por primera vez, estaban caracterizados por la "agrupación en bloques" de trabajos similares. Los modernos sistemas utilizan otras características. El rasgo característico de un sistema por lotes es la ausencia de interacción entre el usuario y el trabajo mientras éste se ejecuta. El trabajo se prepara y se envía. Tiempo después aparece la salida.

3.3.2 Multiprogramación.

Un solo usuario no puede, en general, mantener todo el tiempo ocupado a la computadora o a los dispositivos de entrada y salida. La multiprogramación aumenta la utilización de la computadora organizando los trabajos de manera que ésta siempre tenga algo que ejecutar. El sistema operativo. Escoge uno de los trabajos del depósito y comienza a ejecutarlo. En algún momento el trabajo tendrá que esperar, ya que el sistema ha pasado el control a otro programa y así sucesivamente. Mientras haya otro trabajo por ejecutar, la computadora nunca estará inactiva.

Dentro de los sistemas multiprogramados tenemos tres tipos:

Tiempo compartido.

Utiliza la planificación de la computadora y la multiprogramación para proporcionar a cada usuario, que tiene su propio programa en memoria, una pequeña porción de una computadora de tiempo compartido. La entrada y salida interactiva es demasiado lenta para una computadora por lo que, para que la computadora no permanezca inactiva, el sistema operativo. la cambiará al programa de otro usuario. Esto ocurre tan rápidamente que cada usuario tiene la impresión de que cuenta con su propia computadora, cuando en realidad todos lo comparten.

Tiempo real.

Suele usarse como dispositivo de control en una aplicación dedicada. Tiene restricciones temporales bien definidas, por lo que el procesamiento debe llevarse a cabo dentro de los límites definidos o el sistema fallará. Puede parecernos extraña la utilidad de este tipo de gestión, así que pondremos un ejemplo: una nave espacial se dispone a acoplarse a la estación espacial MIR, nos interesa conocer las coordenadas de la MIR en todo momento para compararlas con las nuestras y así actuar en consecuencia. De nada nos sirve que se resuelvan los cálculos una vez nos hemos estrellado porque un astronauta estaba jugando con la misma computadora al tetris y este consumía toda la potencia de cálculo de la computadora.

Combinados.

Es una mezcla de los dos anteriores. Aunque se ha intentado combinar la funcionalidad del tiempo compartido y el tiempo real en un solo sistema operativo, los resultados han sido pésimos debido a los obvios conflictos entre los requisitos de ambos tipos.

3.3.3 Sistemas distribuidos.

Es un sistema débilmente acoplado, es decir, los procesadores no comparten ni memoria ni reloj, cada uno cuenta con su propia memoria local y se comunican a través de distintas líneas de comunicación. Los procesadores pueden variar de tamaño y función. Las principales ventajas son:

- Compartir los recursos.
- Aceleración de los cálculos.
- Fiabilidad.
- Comunicación.

3.4 Arquitectura de un Sistema Operativo.

Para comenzar este apartado podemos plantear la siguiente pregunta: "¿Qué pasa si el propio sistema operativo necesita hacer algo que es capaz de hacer pero no se encuentra en el código que está ejecutando en ese momento?" Dicho de otra manera, vamos a ver dónde se encuentran las diferentes funciones de un sistema operativo y qué tiene que hacer para usarlas. Hasta ahora hemos visto parte del aspecto "exterior" del sistema operativo, que es la organización que da a los programas a la hora de ejecutarlos. Pasemos a examinar las diferentes posibilidades de implementación de un sistema operativo "por dentro", es decir, no cómo organiza el sistema operativo al resto de programas, sino cómo se organiza respecto a sí mismo.

Kernel monolítico:

La estructura de esta arquitectura es simplemente no tener ninguna. A nivel de núcleo no se produce ninguna abstracción, es decir, si un procedimiento necesita a otro es libre de hacerlo en cualquier momento. Fue el primer enfoque en la historia, el resto son evoluciones.

Microkernel o micronúcleo:

En este caso, el sistema operativo se ocupa solo de unas pocas funciones, reduciendo el núcleo a su mínima expresión. El resto de funciones pasan a estar en el espacio de usuario.

Maquinas virtuales:

El primer sistema con esta arquitectura nació con la idea de separar completamente las dos funciones características de un sistema operativo de tiempo compartido: multiprogramación y un interfaz más apropiado que el del puro hardware. El centro del sistema, también conocido como monitor de la máquina virtual, se ejecuta directamente sobre el propio hardware, encargándose de la multiprogramación. De esta forma, ofrece al nivel superior varias máquinas virtuales, que son copias exactas del hardware, por lo que se puede dar el caso de ejecutar varios sistemas operativos sobre cada una de ellas (de hecho, el caso más usual).

Modelo cliente-servidor:

Esta es la tendencia en cuanto a arquitectura de los sistemas operativos hoy en día. Consiste en reducir al mínimo el kernel, al igual que en el caso de los microkernels, pero en este caso la única función del kernel es de servir de puente entre procesos: cuando una función necesita de otra es el kernel el que se encarga de mantener la comunicación entre ellas, pero nada más.

3.5 Diferentes funciones de un Sistemas operativos.

El sistema operativo crea un entorno para la ejecución de cada proceso, además de ofrecer ciertos servicios a los programas y a sus usuarios. Vamos a ver algunos de ellos.

Los servicios específicos que ofrece cada sistema operativo suelen ser diferentes, dependiendo del sector al que están destinados, aunque algunas clases de ellos son comunes: las operaciones de entrada y salida, la manipulación del sistema de archivos, la detección de errores, etc. Estas funciones tienen el propósito, en su mayoría, de favorecer la tarea del programador, haciendo más fácil su trabajo. Lo que realmente nos está dando el sistema operativo es una capa de abstracción del hardware particular sobre el que corre. Por si no ha quedado claro el porqué de estas facilidades, pongamos un ejemplo: un programador de bases de datos que trabaje con dos computadoras distintas en hardware se encontrará con el problema de que tiene que saber manipular los archivos tanto en una como en otra plataforma. Si el sistema operativo cumple bien el objetivo de abstracción, un mismo programa puede funcionar sobre dos computadoras de arquitectura diferente con el mismo sistema operativo, sin que haga falta modificar el código del programa.

Además de estas funciones, el sistema operativo tiene otro conjunto destinado al funcionamiento eficiente de la computadora: asignación de recursos, gestión de procesos.

3.6 Tipos de llamadas al sistema, o servicios que ofrece el sistema.

Para la gestión de procesos.

Dentro de este tipo nos encontramos todas aquellas llamadas necesarias para la ejecución de programas, así como la eficiente distribución de recursos entre éstos.

Para el acceso a dispositivos:

De entrada y salida: El sistema operativo debe abstraer el funcionamiento del hardware al programador. Para ello, el sistema nos provee de ciertas funciones genéricas para su acceso.

Para la detección de errores y respuesta:

A pesar de ser máquinas, en los sistemas se pueden producir multitud de errores, tanto de software como de hardware, algunos de ellos pueden ser:

- Acceso a zonas prohibidas de memoria (software)
- Imposibilidad de asignar los recursos solicitados por una aplicación (software)
- Fallo de algún dispositivo de almacenamiento (hardware)

En todos los casos el sistema ha de ser capaz de responder con éxito a estos sucesos, o en su defecto, evitar la pérdida de datos.

Para la contabilidad del sistema:

Si bien este tipo de funciones no las encontramos en todos los sistemas operativos, son bastante comunes en aquellos que tienen la particularidad de ser multiusuario.

3.7 Reseña histórica.

A continuación se presenta una tabla cronológica que nos va a ayudar a relacionar diferentes sistemas operativos según sus características más notables.

Tabla de características

Sistema Operativo	Año	Autor	Gestión de procesos	Arquitectura	Multiusuario
Atlas	50-60	University of Manchester	Lotes	monolítico	No
The		Universidad de Eindhoven	Lotes	modular	no
RC4000		Brinch Hansen de Regenecentralen	S.O. Completo	modular	no
Solo		Brinch Hansen de Regenecentralen	multiprogramado	modular	no
CTSS		MIT	multiprogramado-tº compartido	monolítico	si
Multics		MIT	multiprogramado-tº compartido	modular	si
Unix	1969	Ritchie / Thompson	multiprogramado-tºcompartido	monolítico	si
Sprite	1984		multiprogramado	modular	si
Merlin	1984		Lotes	monolítico	no
Windows NT	1985	Microsoft	multiprogramado	modular	si
Mach	1986	Darpa	multiprogramado	monolítico	Si
Amoeba	1994		distribuido	microkernel	Si
Windows 95/98	1995/98	Microsoft	multiprogramado	monolítico	No
Coyote	1996	Trinity College Dublín	distribuido	modular	Si
Exokernel			micro-kernel	monolítico	Si
WindowsNT 3.1	1992	Microsoft	multiprogramado	Monolítico	SI
Windows XP	2001	Microsoft	multiprogramado	Monolítico	SI
Windows Server 2003 family	2003	Microsoft	multiprogramado	monolítico	SI

IV Windows

4 Historia de Windows.

4.1 Windows 1.0

En 1985 Microsoft publicó la primera versión de Windows (Windows 1.0), una interfaz gráfica de usuario (GUI) para su propio sistema operativo (MS-DOS) que había sido incluido en el IBM PC y de computadoras compatibles desde 1981. La interfaz gráfica fue creada después del MacOS de Apple.

Las siguientes fueron las principales características de Windows 1.0:

- Interfaz gráfica con menús desplegadles, no había ventanas en cascada y soporte para ratón.
- Gráficos de pantalla e impresora independientes del dispositivo.
- Multitarea cooperativa entre las aplicaciones Windows.

4.2 Microsoft Windows 2.0

Microsoft Windows 2 salió en 1987, y fue un poco más popular que la versión inicial. Gran parte de esta popularidad la obtuvo de la introducción en forma de versión "run-time" de nuevas aplicaciones gráficas de Microsoft, Microsoft Excel y Microsoft Word para Windows. Éstas podían cargarse desde MS-DOS, ejecutando Windows a la vez que el programa, y cerrando Windows al salir de ellas. Windows 2 todavía usaba el modelo de memoria 8088 y por ello estaba limitado a 1 megabyte de memoria,.

Nacen aplicaciones como Excel, Word for Windows, Corel Drawl, Ami y PageMaker.

Las siguientes fueron las principales características de Windows 2.0:

- Ventanas traslapadas.
- Archivos PIF para aplicaciones DOS.

4.3 Windows 3.0

La primera versión realmente popular de Windows fue la versión 3.0, publicada en **1990**. Ésta se benefició de las mejoradas capacidades gráficas para computadoras de esta época, y también del procesador **microprocesador 80386** que permitía mejoras en las capacidades multitarea de las aplicaciones Windows. Esto permitiría incluso ejecutar en modo multitarea viejas aplicaciones basadas en MS-DOS.

Las siguientes fueron las principales características de Windows 3.0:

- Modo estándar (286), con soporte de memoria grande (large memory).
- Modo Mejorado 386, con memoria grande y soporte de múltiples sesiones DOS.
- Se agregó el Administrador de Programas y Administrador de Archivos.
- Soporte para Red.
- Soporte para más de 16 colores.
- Soporte para cajas de selección, menús jerárquicos y los archivos. INI privados para cada aplicación empezaron a cobrar más valor.

4.4 OS/2 1

Durante la segunda mitad de los 80, Microsoft e IBM habían estado desarrollando conjuntamente OS/2 como sucesor del DOS, para sacar el máximo provecho a las capacidades del procesador Intel 80286. OS/2 utilizaba el direccionamiento hardware de memoria disponible en el Intel 80286 para poder utilizar hasta 16 M de memoria. La mayoría de los programas de DOS estaban por el contrario limitados a 640 K de memoria. OS/2 1.x también soportaba memoria virtual y multitarea.

Este acuerdo pronto fue dejado de lado y la relación entre IBM y Microsoft terminó. IBM continuó desarrollando IBM OS/2 2.0 mientras que Microsoft cambió el nombre de su (todavía no publicado) OS/2 3.0 a Windows NT.

(Microsoft promocionó Windows NT con tanto éxito que la mayoría de la gente no se dio cuenta de que se trataba de un OS/2 reforzado.) Ambos retuvieron los derechos para usar la tecnología de OS/2 y Windows desarrollada hasta la fecha de terminación del acuerdo.

4.5 Windows 3.1 y Windows 3.11

En respuesta a la inminente aparición de OS/2 2.0 , Microsoft desarrolló Windows 3.1, que incluía diversas pequeñas mejoras a Windows 3.0 (como las fuentes escalables TrueType), pero que consistía principalmente en soporte multimedia. Más tarde Microsoft publicó también Windows 3.11 (denominado Windows para trabajo en grupo), que incluía controladores y protocolos mejorados para las comunicaciones en red y soporte para redes punto a punto.

Las siguientes fueron las principales características de Windows 3.1:

- No hay soporte para el modo Real (8086).
- Fuentes TrueType.
- OLE - Object Linking and Embedding.
- Capacidad para que una aplicación reinicie la máquina.
- Soporte de API de multimedia y red.

4.6 Windows NT

Mientras tanto Microsoft continuó desarrollando Windows NT. Para ello reclutaron a Dave Cutler, uno de los jefes analistas de VMS en Digital Equipment Corporation para convertir NT en un sistema más competitivo.

Siendo un sistema operativo completamente nuevo Windows NT sufrió problemas de compatibilidad con el hardware y el software existentes. También necesitaba gran cantidad de

recursos y éstos estaban solamente disponibles en equipos grandes y caros. Debido a esto muchos usuarios no pudieron pasarse a Windows NT. La interfaz gráfica de NT todavía estaba basada en la de Windows 3.1 que era inferior a la Workplace Shell de OS/2.

4.7 Windows 95

En respuesta a ello Microsoft comenzó a desarrollar un sucesor para Windows 3.1 cuyo nombre clave era Chicago. Chicago iba encaminado a incorporar una nueva interfaz gráfica que compitiera con la de OS/2. También se pretendía introducir arquitectura de 32 bits y dar soporte a multitarea preventiva, como OS/2 o el mismo Windows NT. Sin embargo sólo una parte de Chicago comenzó a utilizar arquitectura de 32 bits, la mayor parte siguió usando una arquitectura de 16 bits, Microsoft argumentaba que una conversión completa retrasaría demasiado la publicación de Chicago y sería demasiado costosa.

4.8 Windows NT 3.1

Windows NT 3.1 (la estrategia de marketing de Microsoft era que Windows NT pareciera una continuación de Windows 3.1) apareció en su versión beta para desarrolladores en la Conferencia de Desarrolladores Profesionales de Julio de 1992 en San Francisco. Microsoft anunció en la conferencia su intención de desarrollar un sucesor para Windows NT y Chicago (que aún no había sido lanzada). Este sucesor habría de unificar ambos sistemas en uno sólo y su nombre clave era Cairo. (Visto en retrospectiva Cairo fue un proyecto más difícil de lo que Microsoft había previsto y como resultado NT y Chicago no sería unificados hasta la aparición de Windows XP. Las versiones antiguas de Windows NT se distribuían en disquetes y requerían unos elevados recursos de hardware (además de soportar relativamente poco hardware) por lo que no se difundieron demasiado hasta llegar a Windows NT 4.0 y sobre todo a Windows 2000.

4.9 Windows 95

Microsoft adoptó "Windows 95" como nombre de producto para Chicago cuando fue publicado en Agosto de 1995. Aunque compartía mucho código con Windows 3 e incluso con MS-DOS, Windows 95 tenía dos grandes ventajas para el consumidor medio. Primero, aunque su interfaz todavía corría sobre MS-DOS, tenía una instalación integrada que le hacía aparecer como un solo sistema operativo: uno ya no necesitaba comprar MS-DOS e instalar Windows encima. Segundo, introducía un subsistema en modo protegido que estaba especialmente escrito a procesadores 80386 o superiores, lo cual impediría que las nuevas aplicaciones Win32 dañaran el área de memoria de otras aplicaciones Win32. En este respecto Windows 95 se acercaba más a Windows NT, pero a la vez, dado que compartía código de Windows 3.x, las aplicaciones podían seguir bloqueando completamente el sistema en caso de que invadieran el área de aplicaciones de Win16.

4.10 Windows NT 4.0

Después de la aparición de Windows 95, Windows NT continuaba usando la interfaz de Windows 3.1. Entonces Microsoft publicó Windows NT 4.0 que tenía la nueva interfaz de Windows 95 pero sobre Windows NT. Cabe comentar, que apareció un añadido para Windows NT 3.5 que permitía disponer de dicha interfaz, pero no venía incluido de serie.

4.11 Windows 98

El 25 de Junio de 1998 llegó Windows 98, que era una revisión menor de Windows 95. Incluía nuevos controladores de hardware y el sistema de archivos FAT 32 que soportaba particiones mayores a los 2 GB permitidos por Windows 95.

4.12 Windows 98 Second Edition

En 1999 Microsoft sacó al mercado Windows 98 Second Edition, que su característica más notable era la capacidad de compartir entre varios equipos una conexión a Internet a través de una sola línea telefónica.

4.13 Windows Millennium Edition

En 2000 Microsoft introdujo Windows ME que era una copia de Windows 98 con más aplicaciones añadidas. Windows ME fue un proyecto rápido de un año para rellenar el hueco entre Windows 98 y el nuevo Windows XP. En teoría Windows 2000 iba a ser la unificación entre las dos familias de Windows, la empresarial y la de hogar, pero por retrasos, se lanzó este pequeño avance. En esta versión se aceleraba el inicio del sistema y oficialmente ya no se podía distinguir entre el MS-DOS y el entorno gráfico (aunque aparecieron parches que permitían volver a separarlo como se hacía con versiones anteriores).

4.14 Windows 2000

En este mismo año vio la luz Windows 2000, una nueva versión de Windows NT muy útil para los administradores de redes y con una gran cantidad de servicios de red y lo más importante: comenzaba a soportar dispositivos Plug&Play que hasta el momento venían siendo un problema con Windows NT.

4.15 Windows XP

La unión de Windows NT/2000 y Windows 3.1/95/98/SE se alcanzó con Windows XP liberado en 2001 en su versión Home y Professional. Windows XP usa el kernel o núcleo de Windows NT. Incorpora una nueva interfaz y hace alarde de mayores capacidades multimedia, seguridad, etc. Como inconvenientes, deja atrás la posibilidad de configurar tarjetas de expansión que no sean Plug&Play.

4.16 Windows CE

Microsoft Windows CE es una plataforma de sistema operativo para un amplio rango de dispositivos computacionales móviles. La plataforma Windows CE hará posible que nuevas categorías de dispositivos que no sean computadoras puedan comunicarse unos con otros, compartir información almacenada en computadora basados en Windows, y conectarse a Internet. Los primeros productos basados en Windows CE, los Handheld PCs (computadora de bolsillo).

Windows CE es un sistema operativo nuevo, compacto y portadle, construido desde las bases para posibilitar el desarrollo de un gran número de dispositivos comerciales y hogareños, incluyendo computadoras de Bolsillo (Handheld PC), "wallet PC", dispositivos inalámbricos tales como teléfonos celulares inteligentes, y la próxima generación de consolas de video juego incluyendo reproductores de DVD.

El sistema operativo Windows CE es un sistema de 32 bits, multitarea y multihilado que tiene una arquitectura abierta, otorgando un soporte a una variedad de dispositivos.

Windows CE hace posible que se generen nuevas categorías de productos que pueden "hablar" unos con otros, compartir e intercambiar información con computadoras basadas en Windows, y comunicarse con una amplia variedad de sistemas empresariales o con Internet para el acceso al correo electrónico y a la World Wide Web.

V Técnicas de protección

5.1 Control de accesos por computadora.

5.1.1 Identificadores.

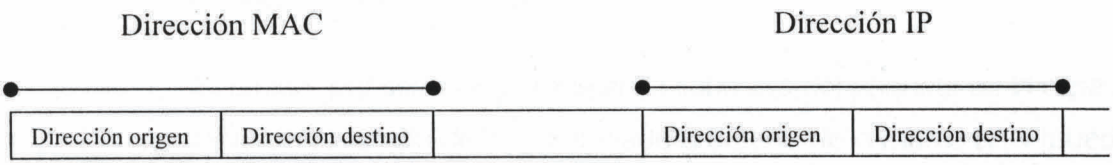
Este tipo de control a partir de la computadora utiliza para acceder. Por lo tanto, se deben poder identificar las computadoras y diferenciarlas y, si es posible, agruparlas en familias. Una computadora se puede identificar por:

- Numero de serie del procesador.
- Dirección MAC.
- Dirección IP o de otro protocolo de red.
- Nombre Internet.

El número de serie de la computadora no se utiliza normalmente. En general los procesadores no tienen números de serie accesibles por el software excepto algunas computadoras.

En las computadoras se utilizan los números de serie en el control de venta o actualizaciones de software asignado a una computadora, así se evita la piratería informática. Este sistema también se puede realizar con la dirección MAC y IP, pero entonces se puede cambiar de computadora.

Los únicos datos que viajan en los paquetes son las direcciones MAC y las direcciones IP de la computadora origen (emisora) y destino (receptora) como se indica en la figura siguiente. Así son los únicos identificadores que pueden utilizar legalmente los filtros.



Identificadores de paquetes

5.1.2 Filtros por dirección MAC.

Las direcciones MAC identifican las computadoras para los protocolos de enlace de las redes LAN. Así estas direcciones están en los paquetes de los protocolos de LAN: Ethernet, Token Ring, ATM, FDDI, etc.

Las desventajas de este método son:

- Números difíciles de tratar.

La asignación de la dirección se hace por Hardware, o sea vienen programadas en las tarjetas de red, excepto raras excepciones. Todas las direcciones son únicas en el mundo pero sus valores no tienen más relación entre ellas que el proceso de fabricación, por lo tanto, las direcciones MAC de las tarjetas de las computadoras de una empresa no tienen ninguna característica común.

- Sólo se puede utilizar en el entorno de la LAN.

Solo se utilizan dentro del entorno de una LAN, o sea, una red de Hubs y Switchs, así cambian cuando pasan por un Router y no existen en las computadoras aisladas conectas telefónicamente a Internet. No se puede realizar control a nivel WAN.

- No pueden discriminar entre servicios.

No se puede discriminar por servicios porque en la cabecera del paquete de la capa MAC no hay información del servicio, solo de la computadora destino de la misma LAN (puede ser un Rauter).

- Solo se pueden realizar desde filtros.

Las aplicaciones no tienes acceso a la dirección MAC del paquete que llega, a menos que actúen por debajo del sistema operativo, que no es normal. Así esta forma de control siempre se realiza en la red mediante los equipos de interconexión, los Swintchs y sistemas de VLAN.

- Siempre son bidireccionales.

No permiten controles unidireccionales

Las ventajas son:

- Método difícil de atacar.

Es muy difícil falsificar la dirección del paquete. Además no se puede cambiar por software.

- El filtrado es muy rápido

Como actúan a nivel dos, el filtrado se hace con elementos Hardware y, por lo tanto, es muy rápido.

Se utilizan poco y para cosas especiales donde la separación entre las dos áreas quiere ser total y sin unidireccionalidad.

5.1.3 Filtrado por nombre o dirección de red y puerto.

Estos filtrados se realizan prohibiendo el acceso de una computadora identificada por una dirección IP o un nombre. Así se permite realizar un control de acceso a cada servicio.

Tratar con nombres de Internet es mas sencillo por que son mas fáciles de recordar y tratar, pero también el inconveniente de que el nombre no viaja con el paquete. Así cuando el sistema de control filtra solo conoce la dilección IP de la computadora que envió el paquete. Para saber el nombre debe preguntar a un servidor de nombres (DNS) mediante el protocolo de DNS inverso. Esto debilita la seguridad porque introduce un elemento mas para romper por el atacante, se puede modificar temporalmente la información del DNS o suplantar su mensaje de respuesta.

La dirección IP y los nombres son mucho más manejables que las direcciones MAC. Se actualizan por software y siempre obedecen a una lógica. Los nombres son elegidos por la empresa y, por lo tanto, están relacionados. Las IPs se agrupan por clases o subclases ligadas a una empresa, una zona geográfica o cualquier grupo, así es fácil realizar filtros que afecten a todo un grupo de computadoras de la misma zona sin necesidad de introducir las direcciones una a una. Los grupos de direcciones IP afines se definen con las mascaras.

Así los filtros de IP se pueden definir prohibiciones o permisos con las siguientes posibilidades:

Maquina/s origen	Maquina/s destino	Prohibiciones o permisos de
IPx.x.x.x	IPx.x.x.x	Acceso completo de origen a destino
IPx.x.x.x Mascarax.x.x.x	IPx.x.x.x	Acceso completo del grupo de maquinas origen a destino.
IPx.x.x.x Mascarax.x.x.x	IPx.x.x.x Mascarax.x.x.x	Acceso completo de grupo origen al grupo destino
IPx.x.x.x	IPx.x.x.x Puerto y	Acceso de origen a un servicio de destino.
IPx.x.x.x Mascarax.x.x.x	IPx.x.x.x Puerto y	Acceso del agrupó de maquinas origen a un servicio de destino
IPx.x.x.x Mascarax.x.x.x	IPx.x.x.x Mascarax.x.x.x Puerto y	Acceso un grupo de maquinas origen a un servicio del grupo destino

El control se puede hacer desde el servidor o desde un filtro intermedio (Router o Firewall).

5.1.4 Filtros con Routers o Firewalls

Muchos Routers permiten crear filtros de IP y mascaras origen a IP, mascara y puerto destino.

Los Firewallas realizan funciones mas avanzadas, permiten filtrar mirando características de la capa de transporte.

El protocolo TCP es orientado a conexión, por lo tanto, antes de la transmisión de información de realizar una apertura de sesiones correctas y la finaliza un cierre de sesión correcta se realiza mediante 3 mensajes. Los Firewalls únicamente controlan los paquetes de conexión que se diferencian de los otros por que el bit de ACK a '0'. Con este procedimiento se consiguen dos mejoras:

- Mas velocidad porque el Firewall solamente examina un paquete de cada sesión.
- Unidireccionalidad en los casos de filtros para grupos de puertos.

Cuando el filtro se programa para prohibir el acceso a un puerto determinado normalmente no hay problemas de direccionalidad porque el puerto utilizado como cliente no es el mismo que el utilizado como servidor.

Los protocolos UDP e ICMP no son orientados a conexión, se envía información sin necesidad de haber abierto una sesión anterior. Por lo tanto no se puede controlar los primeros paquetes, o se controlan todos o no se controla ninguno. Para evitar problemas de direccionalidad se utiliza la técnica de inspección de estado. Cuando se filtra con inspección de estado en principio se permite el paso, pero se gurda memoria de los maquetes que van pasando entre las dos computadoras para cada par de puertos. Así conociendo toda la historia de la comunicación y con la inteligencia de un firewall puede detectar si se realiza algún ataque y cortar si es necesario.

En algunos servicios, como FTP o los que utilizan RPCs, el servidor utiliza puertos distintos en cada conexión. El cliente realiza siempre la primera conexión al mismo puerto pero durante la transmisión el servidor puede utilizar otros puertos para sesiones concretas, este puerto es comunicando al cliente durante el traspaso de información por el puerto inicial.

5.1.5 Ataques al control por IP o nombre.

Existen diversos ataques al control de acceso por IP o nombre. Algunos se saltan el control para acceder a la información restringida y otros están fuera del alcance de los filtros. Se agrupan en:

- Spoofing. Consiste en cambiar la dirección origen por una que es aceptada por el filtro.
- Hijacking. Consiste en secuestrar una sesión, es decir, introducir en la comunicación aprovechando una sesión que ha abierto un usuario con privilegios. Se deben enviar los mensajes con la IP del usuario que abrió la sesión y recibir las respuestas del servidor antes que el usuario legal.
- Tunneling. Se aprovecha una computadora que esta detrás del filtro o tiene permisos de acceso para utilizarlo de plataforma. La computadora externa recibe una conexión de la interna y a partir de esta realiza los ataques. También se puede hacer utilizando una

conexión permitida la computadora interna y desde ésta pasar a un software capaz de atacar. Para ello se necesita la colaboración de algún usuario interno, poder instalar un caballo de Troya que abra un camino o utilizar un error (bug) de un programa inocente.

- Ataques al DNS. Modificar las memorias caches del DNS falsificando las relaciones IP/nombre, así cuando el filtro pregunte a que nombre pertenece una IP que pide permiso de entrar se consigue que el DNS conteste un nombre autorizado.

5.2 Control de acceso de usuario.

5.2.1 Características generales.

Para realizar la selección de usuario se debe hacer una identificación única del usuario o grupo de usuarios, debe ser independiente de la computadora utilizada y el sistema de telecomunicanicacion. A continuación se mencionarán tres métodos para identificar personas:

- Por las características físicas: biométricos.
- Por un secreto compartido: contraseñas (Passwords).
- Por la posesión de un objeto (software o hardware): token o certificados digitales.

Los sistemas mas utilizados actualmente son de contraseña, con diferentes variantes se aplican a casi todos los aspectos de la seguridad de la informática. Los sistemas biométricos son mucho más nuevos pero se están desarrollando a gran velocidad.

Los sistemas de posesión de un objeto son los mas antiguos en control de accesos físicos, la llave de las puertas o los sellos de los reyes son tan antiguos como el concepto de acceso o identificación de derechos. Pero el mundo digital se utilizan muy poco para el acceso a sistemas de información, probablemente por el gasto extra que supone un identificador de objetos. Se están desarrollando muchos los accesos por sistemas criptográficos llamados certificados digitales

Igualmente todos los sistemas se pueden confiar para aumentar la seguridad, especialmente el uso de contraseñas normalmente acompaña a los sistemas biométricos y los objetos.

El control de acceso por usuarios también se puede clasificar por la ubicación del filtro, así puede estar en:

- Servidor. Permite control de acceso remoto y local.
- Filtro de la red. Solo controla accesos remotos

Por ultimo, el control de accesos por usuario se puede clasificar atendiendo a quien organiza este control. Existen tres tipos de organización:

- DAC (Discretionary Access Control)

El creador del archivo define los permisos de los objetos (archivo, recursos, etc.). Desde la administración del sistema se pueden crear grupos de usuarios, usuarios genéricos y varios tipos de facilidades para que el creador del archivo pueda asignar los permisos. Es el control más habitual en los sistemas operativos: Windows de Microsoft, UNIX, etc. Es muy vulnerable a los caballos de Troya.

- MAC (Mandatory Access Controls)

La administración del sistema operativo asigna los permisos a los objetos. El sistema operativo crea un numero de etiquetas (secretas, confidencial, no calificada, etc.) con unos derechos de acceso asignados y cada objeto tiene sus etiquetas. Los usuarios se agrupan en sujetos que tienen unos permisos debidos para cada etiqueta. Una protección buena contra caballos de Troya es hacer que cada nivel pueda escribir a los archivos de su nivel o superior y leer en los de su nivel inferior.

- RBAC (Role Based Access Controls)

Intenta tener las ventajas de los anteriores sistemas y evitar la rigidez del MAC y la inseguridad del DAC. El funcionamiento por roles se acerca mas a la distribución de trabajos real de las empresas. Los roles son funciones concretas que realiza un usuario dentro de la empresa

durante un tiempo determinado, así a los usuarios se les asigna unos roles y cada rol tiene unos permisos sobre los objetos.

5.2.2 Control por contraseñas.

Las contraseñas son un punto débil de los sistemas de seguridad, pero para realizar control de acceso por usuario son el sistema más sencillo, popular y probado. Se puede hacer una aproximación con las protecciones físicas de los edificios, puertas y su sistema de abertura (llaves, combinaciones, la cerradura) son imprescindibles pero también son el principal método utilizado para acceder sin permiso.

En los sistemas operativos y las aplicaciones con filtro las contraseñas no pueden tener permisos de usuarios restringidos ya que al entrar la contraseña el usuario puede ser cualquiera. Una forma de evitar este problema seria dar permiso de administrador al archivo y que el usuario por defecto cuando se introdujera la contraseña fuera el administrador, pero esto seria muy peligroso porque cualquiera tendría permiso de administrador por un momento.

Así este archivo sin permisos en principio es accesible por todos los usuarios, pero se utilizan técnicas para evitar este acceso. Un ejemplo en Windows de Microsoft el archivo se esta utilizando siempre por el sistema y los archivos que utiliza el sistema no son accesibles para escritura, esta protección ya ha sido vencida por los programas de los atacantes.

Si los archivos son accesibles, el atacante únicamente necesita desencriptar las contraseñas. Para hacer difícil esta tarea se utilizan sistemas de encriptación irreversibles y además, el descubrimiento de una contraseña no da pista sobre las otras. Un ejemplo de encriptación seria el siguiente:

Los servidores Windows NT permiten dos formas de codificar las contraseñas, la forma propia y la de LANManager, esta última solo se utiliza para compatibilidad con las redes de este tipo.

Aquí se menciona la propia de Windows NT.

En Windows NT se ha buscado dar más velocidad al proceso a costa de utilizar criptografía débil. Como los atacantes no intentan romper el algoritmo de encriptación sino que lo utilizan para probar contraseñas, este sistema no basa su seguridad en la fortaleza del algoritmo, cosa que es discutible. Se consigue una velocidad mucho más alta que en UNIX, esto proporciona comodidad al usuario pero también facilita el trabajo del atacante.

El sistema es:

a.m.[Hash[contraseña]]

La función Hash utilizada fue en principio MD4. También cumple las propiedades de ser:

- Irreversible porque las funciones Hash siempre son irreversibles.
- El conocimiento de una contraseña y su encriptación no da información para descubrir las otras.

Permite frases largas como contraseña (Passphrase) ya que las funciones Hash resumen textos de cualquier longitud variable.

5.2.3 Ataques a contraseñas.

Las contraseñas son un punto muy vulnerable de la seguridad del sistema de información, si el atacante consigue esa secuencia de pocos caracteres que forma la contraseña tiene la puerta abierta a tacar cualquier recurso. Las formas de poder descubrir las contraseñas de los usuarios se pueden agrupar en:

- Con acceso al archivo.

Si se tiene acceso al archivo de contraseñas adivinarlas es solo cuestión de tiempo. Para ello se utilizan programas denominados Crackers que prueban todas las posibilidades hasta encontrar una que al encriptarse coincide. Hay dos métodos de elegir las posibles palabras:

- Diccionario. Prueban todas las palabras que pueden aparecer en una enciclopedia, o sea nombres comunes (de un diccionario), nombres de persona, de animal, geográficos, fechas, números, etc. Esto se puede hacer consecutivamente para varios idiomas y, además, ir haciendo pasadas intercalando numero y signos de puntuación. Para que una contraseña sea fácilmente recordable debe ser clara para el usuario, por lo tanto, ser alguna palabra con significado. Pero este hecho reduce mucho el numero de posibilidades, con 8 caracteres se pueden formar 128^8 = $7{,}2*10^{16}$ palabras mientras en las enciclopedias hay solo unos centenares de miles de palabras.
- Prueba y ensayo (Task Force). Se prueban todas las combinaciones de letras, números y signos posibles. Este método es mucho más lento que el anterior pero al número de caracteres de forma progresiva.

- Caballos de Troya.

Se sustituyen programas útiles por aplicaciones por el atacante que tienen el mismo nombre. Los ejecutan el propio usuario pensando que es un programa y realizan funciones de observación, modificando o destrucción de la información. Los caballos de Troya sirven para muchos tipos de ataques, uno concreto es la captura de contraseñas. Se puede hacer sustituyendo uno de los programas que tratan las contraseñas en claro, capturando el teclado o capturando las transmisiones por la red si se envía en claro.

- Espías de la red.

Si se instala en una computadora un programa llamado sniffer, este captura toda la información que circula por la Ethernet o Token Ring de la computadora. Estos programas descubren las contraseñas mientras circulan por la red. Si no están encriptadas (hay muchos sistemas que no encriptan las contraseñas para enviarlas), el atacante ya ha conseguido su medio de acceso. Pero si están encriptadas también los pueden utilizar repitiendo el mensaje como respuesta a una petición de identificación. El atacante únicamente necesita poder instalar en el servidor o en una computadora de la misma LAN un programa de este tipo.

- Ingeniería social.

Uno de los sistemas mas utilizados es el llamado por los atacantes ingeniería social, no es técnico sino que se basa en descubrir las contraseñas directamente de los usuarios. Los métodos pueden ser observar el teclado cuando se introduce la contraseña, descubrirlo escrito en un papel, pedirlo por correo electrónico o teléfono haciéndose pasar por el administrador, etc. Las estadísticas dicen que es uno de los sistemas mas utilizados.

5.2.4 Defensas a ataques a contraseñas.

Para defenderse de estos ataques se puede trabajar en tres líneas:

- Políticas de personal.
- Herramientas de programas.
- Sistemas de contraseña de un uso.

Las políticas de personal van orientadas a aconsejar u obligar al personal de la empresa a cumplir ciertas normas para proteger sus propias contraseñas. Tanto los ataques con acceso al archivo como los de ingeniería social se basan en aprovechar que los usuarios no tienen cuidado con la elección y el mantenimiento de sus contraseñas. Una política puede fijar normas como:

- Tamaño mínimo.
- Intercalar entre las letras números y signos de puntuación.
- Prohibir password de diccionario.
- Cambiarlo cada cierto tiempo.
- Si un atacante entra utilizando el password de un usuario, sancionarlo.

Las herramientas pueden ser opciones del sistema operativo, programas complementarios al sistema o programas de inspección. Los objetivos son:

- Obligar por software a cumplir las políticas de personal.
- Atacar con un Cracker u otro programa para probar la resistencia del sistema de contraseñas.
- Cancelar cuentas que han recibido intentos de acceso fallido. Se recuperan después de un tiempo o través del administrador.

Una manera de aumentar mucho la seguridad en los accesos remotos es utilizar unos sistemas, llamados OTP (One Time Password), donde la contraseña de un usuario cambia cada vez que se usa, o sea, contraseñas de un uso. El servidor y el usuario deben estar sincronizados para saber en cada momento que contraseña se debe utilizar. Si algún atacante descubre una contraseña no le sirve porque para el siguiente acceso se necesita otra.

Los sistemas OTP necesitan servidores preparados para calcular cada vez la contraseña que toca y clientes con un software o un equipo electrónico capaz de realizar la misma función. Estos quipos electrónicos se llaman testigos (Tokens) y se pueden considerar de la familia de control de accesos por posesión de un objeto combinado con contraseñas.

En OTP para calcular la contraseña se utilizan los siguientes parámetros:

- Una frase secreta del usuario (Passphrase).
- Una palabra aleatoria conocida por el servidor y el software o hardware del usuario.
- Una función Hash.
- El número de accesos se han realizado desde el inicio, o sea, el número de secuencia.

Así se entra a una función Hash la passphrase y la palabra aleatoria, al resultado se le aplica varias veces la misma función Hash según marca el número de secuencia. El resultado se envía al servidor como contraseña, este realiza el mismo proceso y se comparan los resultados.

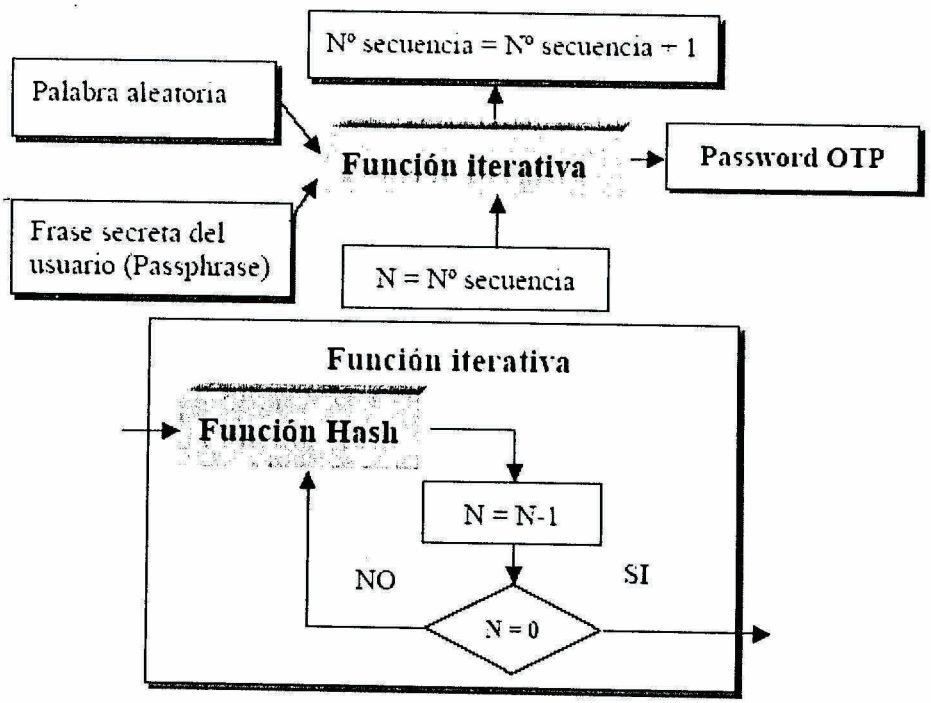


Figura de Algoritmo de una OTP

5.2.5 Sistemas biométricos.

Estos sistemas utilizan una característica física del usuario (autentificadores). La característica debe de ser única en las personas y no cambiar con las circunstancias (estado de ánimo, temperatura ambiente, iluminación etc.) ni con el tiempo (insensible al envejecimiento). Estos sistemas son mucho mas seguros que los de contraseña sobre todo si se combinan con otros, como ventajas tienen:

- Intransferibles. El atacante no los puede utilizar aunque los conozca. Esta característica es suficiente para considerar el sistema mejor que los de contraseña o posesión de objetos.

- No necesitan gestión del usuario, como cambiarlos a menudo, recordar frases largas, guardar objetos (Tokens), etc.
- Sirve tanto para accesos físicos como lógicos.
- Son muy seguros a cualquier ataque.

Algunas de las desventajas:

- Necesita electrónica adicional para realizar las lecturas de imágenes y, por lo tanto, son más caros.
- La tecnología no esta muy avanzada.
- Hay algún prejuicio moral porque las características físicas de la personas son invariables y hacerlas publicas implica estar fichado para toda la vida
- No son exactos.

La mayoría de estas desventajas se corregirán con el tiempo.

En una identificación biométrica se realizan las siguientes fases:

- Captar la imagen o sonido relativo al autentificador de la persona mediante un sensor.
- Modificar los datos brutos de la imagen o sonido mediante técnicas de tratamiento de señal para extraer los parámetros básicos y únicos del usuario (modelos/patrones), así como eliminar los datos dependientes de las condiciones externas de la medida.
- Comparar estos parámetros con los almacenados.

Como se puede deducir del proceso, la comparación de resultados nunca es exacta, por lo tanto se busca un grado de aproximación a partir del cual se considera que los parámetros medidos son de la misma persona que los almacenados. Así es posible tener errores, estos están medidos estadísticamente para cada método biométrico con los siguientes índices:

- FAR (False Acceptence Rate). Mide en tanto por ciento la relación de identificaciones erróneas consideradas correctas.
- FRR (False Rejec Rate). Mide en tanto por ciento la relación de rechazos al acceso que eran correctos.

- SR (Succes Rate). Da un índice global de la calidad del sistema, relacionando los índices anteriores, se utiliza la formula: SR = 100 – (FAR + FRR).

En el proceso de comparación se pueden diferenciar en dos métodos: identificación y verificación.

La identificación consiste en encontrar en una base de datos de parámetros biométricos si los medidos coinciden aproximadamente con algún usuario, es para un sistema de acceso donde no se introduce el nombre de usuarios o para búsqueda de personas (por ejemplo en archivos policiales).

La verificación compara directamente los parámetros medidos con los del usuario y según la aproximación matemática se considera el acceso permitido o denegado, es el sistema de acceso más habitual. Lógicamente la certificación tiene índices de FAR y FRR mucho más de elevados que la identificación.

Los sistemas biométricos actuales se basan en medidas de:

- Emisión de calor.

Se mide la emisión de calor del cuerpo o termograma, realizando un mapa de valores sobre la forma de la persona. Permite medidas sin contacto, o sea, a distancia.

- Huella digital.

Aprovecha las características diferentes entre todas las huellas digitales de los humanos. Necesita un escáner de dedos.

- Mano.

Es fácil de implementar y tiene un costo bajo. El problema es que varía mucho con el tiempo y las condiciones físicas de la persona. Los patrones se deben renovar de vez en cuando.

- Caras.

Debe medir características únicas e invariables con el tiempo y las expresiones de las caras, como la distancia entre los ojos, de la boca a la nariz, etc.

- Iris.

El iris de los ojos presenta multitud de líneas concentradas que son diferentes en todos los humanos. Un inconveniente es el rechazo social a colocar el ojo delante de un escáner. Es un sistema lento porque maneja muchos datos pero tiene mucha exactitud.

- Retina.

Este sistema tiene un FAR de 0 pero un FRR del 12%, por l tanto se puede utilizar para sistemas donde es muy importante evitar el acceso de atacantes.

- Voz.

Se graba la dicción de una frase, siempre la misma, por el usuario y en los accesos se compara la voz. Es muy sensible a factores externos como el ruido de fondo, el estado de ánimo o el envejecimiento pero tiene la ventaja de no necesitar contacto y utilizar sensores muy baratos y habituales en las computadoras (micrófonos), para acceso físico en lugares públicos tiene rechazo social. Es el único con posibilidad de transferirse ya que los atacantes pueden hacer una grabación externa sin ser vistos. Una ventaja es la posibilidad de verificación telefónica.

5.2.6 Acceso con objetos físicos: Tokens.

Los Tokens son objetos utilizados para el control de acceso de usuarios. Pueden ser:

- Memorias. Guardan una palabra clave, contraseña. La ventaja es poder utilizar contraseñas aleatorias sin necesidad de recordarlas.

- Inteligentes. Son equipos electrónicos que realizan un algoritmo donde se crean contraseñas de uno (OTP) o se generan un protocolo entre el servidor y el token (certificado).

Pueden estar contenidos en:

- Tarjetas magnéticas. Solo permiten memoria, se necesita un lector magnético.
- Tarjeta chip. Tiene un procesador interno que permite inteligencia. Se necesitan lectores especiales.
- Memorias EPROM o Flash. Se introducen en llaveros o otros objetos pequeños y permiten almacenar contraseñas sin inteligencia.
- Calculadoras. Son pequeñas computadoras que permiten inteligencia. Se comunican con el usuario mediante teclados, displays y/o conexiones seria a la computadora.

Estos sistemas complementan otros sistemas de acceso: contraseñas, biométricos o certificados digitales. Así su función es reforzar los otros, por lo tanto, aumentan mucho la seguridad porque añaden el factor de posesión de un objeto.

El problema puede ser el robo o la perdida del Token, para solucionar esto se deben combinar con la entrada de una contraseña o una medida biométrica.

5.2.7 Acceso con certificados digitales

Este sistema utiliza criptología para dar un objeto lógico, no físico, a los usuarios con permisos. Esta protegido contra robo, perdidas y repetición de mensajes porque el proceso de acceso incluye un protocolo de validación.

Un usuario autorizado debe tener:

- Una clave privada de algún algoritmo asimétrico.

- Un certificado digital con la clave pública pareja de la privada y firmado digitalmente por el servidor.

El certificado digital es un objeto lógico (código) que contiene:

- Nombre y datos del usuario.
- La clave publica del usuario.
- Datos e informaciones generales.
- La firma digital de una tercera persona.

Esta tercera persona asegura que la clave pública es de quien dice ser. Así la seguridad se basa en la corrección de la firma digital de la tercera persona.

Una firma digital se realiza haciendo el resumen del texto y encriptandolo con la clave privada de firmante. Así al desencriptarlo con la pública y comparando con el resumen otra vez calculado puede comprobarse que:

- El texto no ha sido modificado porque los resúmenes coinciden.
- La firma es de la persona que tiene la clave privada pareja de la pública utilizada para desencriptar.

El sistema de acceso con certificados digitales se basa en las siguientes fases:

- El usuario autorizado ha recibido un certificado digital con su nombre y su clave publica firmado por el servidor donde quiere acceder. también ha recibido de manera secreta la clave privada.
- Para acceder envía su certificado.
- El servidor comprueba la firma del certificado y guarda la clave publica.
- El servidor envia un número aleatorio.
- El usuario encripta el numero aleatorio con su clave privada y envía resultado.

- El servidor desencripta y comprueba que la clave privada es pareja de la pública pero ha llegado con el certificado.

El proceso puede complicarse pero siempre se debe basar en los mismos principios:

- La posesión del certificado digital correctamente firmado implica que este usuario tiene la clave privada pareja de la pública indicada y la ha recibido del servidor.
- La posibilidad de encriptar con la clave privada indica que la persona que han robado por la red el certificado.

Un problema es como dar de baja usuario. Para esto se utiliza:

- Todos los certificados tienen fecha de caducidad.
- Listas de revocación de certificados (CRL). Si se quiere dar de baja un certificado y no esta caducado se añade a la CRL hasta que caduque.

Los certificados son como el carnet de identidad de las personas, por lo tanto implican mucha gestión del servidor. Así si el servidor quiere activar un grupo de usuarios con cada usuario. Además también se deben gestionar las bajas y la entrega de las claves privadas de una manera segura. Además para un usuario con varios accesos también puede representar una compilación tener que gestionar diversas claves privadas y certificados. La solución a estos problemas es un sistema llamado certificados de atributos.

La certificación de atributos añade una filosofía nueva universal para la seguridad y los controles de acceso. El certificado individual de una persona física o jurídica debe ser como el carnet de identidad. Se debe asignar por una entidad que ofrece confianza a todo el mundo este certificado no sirve para acceder pero si para identificar al usuario delante de cualquiera. El formato del certificado individual deberá ser estándar para todo el mundo y las entidades que los emiten y firman reconocidas por todo el mundo. Para aplicaciones concretas, como el control de accesos, se utilizan certificados de atributos que tienen las siguientes características:

- Explican atributos concretos de la persona física o jurídica. Por ejemplo: pertenecer a una empresa, tener una nacionalidad, no estar fichado, ser solvente, estar de alta en el acceso a

una Web, formar parte de un grupo con permisos de acceso, etc. estos atributos son los que interesan para acceder a recursos.

- Tiene una duración muy corta y se han de estar renovando continuamente. Así se evita la gestión de las CRL.
- Tiene forma libre y puede ser expedidos por cualquiera.
- Siempre se entregan con el certificado personal que avala la persona propietaria de los atributos. Es como presentar a la entrada de un club un carnet de socio (sin fotografía) y el carnet de identificación para asegurar la identidad personal.

¿Cómo trasportar el certificado? Si siempre se accede desde la misma computadora se puede grabar en el disco, pero en control de accesos por usuario siempre se intenta dejar al usuario libertad de computadora. La solución es utilizar Tokens (en concreto tarjetas de chip) donde se almacenan los certificados y se implementa el protocolo.

VI Criptografía

5 Introducción.

La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales su fin es que sólo las personas autorizadas lo puedan entender el mensaje.

Desde sus inicios, la criptografía llegó a ser una herramienta muy usada en el ambiente militar, en la segunda gran guerra tuvo un papel determinante, una de las máquinas de cifrado y que tubo gran popularidad se llamó ENIGMA. Al terminar la guerra las agencias de seguridad de las grandes potencias invirtieron muchos recursos para su investigación. La criptografía como la conocemos hoy surgió con la invención de la computadora.

La criptografía actual se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como DES (Data Encryption Standard) en 1976 que se da a conocer mas ampliamente, principalmente en el mundo industrial y comercial. Posteriormente con el sistema RSA (Rivest, Shamir, Adleman) en 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación de satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión etc.

6.1 Ramas de la criptografía.

La criptografía se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica, DES pertenece al primer grupo y RSA al segundo.

6.2 Problemas de seguridad que resuelve la criptografía.

Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas.

Ejemplos: Si la comunicación se establece por teléfono y alguien intercepta la comunicación o escucha la conversación por otra línea podemos afirmas que no existe privacidad. En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto si ciframos (escondemos) la información cualquier intercepción no autorizada no podrá entender la información confidencial. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Ejemplos: Cuando compramos un boleto de avión es muy prudente verificar que los datos son los correctos antes de terminar la operación, en un proceso común esto se puede realizar al mismo tiempo de la compra, por Internet como la compra se puede hacer desde dos ciudades muy distantes y la información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control. Es muy importante estar seguros que la información transmitida no ha sido modificada (en tal caso se dice que hay integridad). Esto también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos.

La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

Ejemplos: las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usando quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, y de algún modo reemplaza a la firma autógrafa que se usa comúnmente, para certificar mensajes se usa criptografía simétrica.

Por Internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.

Cuando se diseña un sistema de seguridad una gran cantidad de problemas puedes ser evitados si se ponen en función de comprobar autenticidad, de garantizar privacidad, de asegurar integridad y evitar el no rechazo.

La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las claves y la legislación adecuada resuelven satisfactoriamente los anteriormente problemas planteados.

VII Criptografía simétrica y asimétrica

7.1 Criptografía Simétrica.

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía es conocida también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias:

La criptografía simétrica de bloques (block cipher).

La criptografía simétrica de lluvia (stream cipher).

La criptografía simétrica de resumen (hash functions).

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, e inversamente, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.

La criptografía simétrica ha sido la más usada en toda la historia, ésta a podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

7.1.2 DES.

Es un sistema criptográfico que toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, con una clave de 56 bits. Este sistema fue tomado como estándar y ha sido uno de los más conocidos, usados y estudiados.

DES opera con una llave de longitud de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usada como de paridad, pero en si la clave solo tiene 56 bits de longitud. Dependiendo de la naturaleza de la aplicación.

DES tiene 4 modos de operación para poder implementarse: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit ó byte por byte y el OFB (Output Feedback Mode) el mismo uso pero evitando propagación de error.

En los últimos 20 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: TDES, RC-5, IDEA, FEAL, LOKI'91, DESX, Blowfish, CAST, GOST, etc. Sin embargo no han tenido el alcance de DES, a pesar de que algunos de ellos tienen mejores propiedades.

Entre los ataques más potentes a la criptografía simétrica están el criptoanálisis diferencial y lineal, sin embargo no han podido ser muy eficientes en la práctica por lo tanto, por el

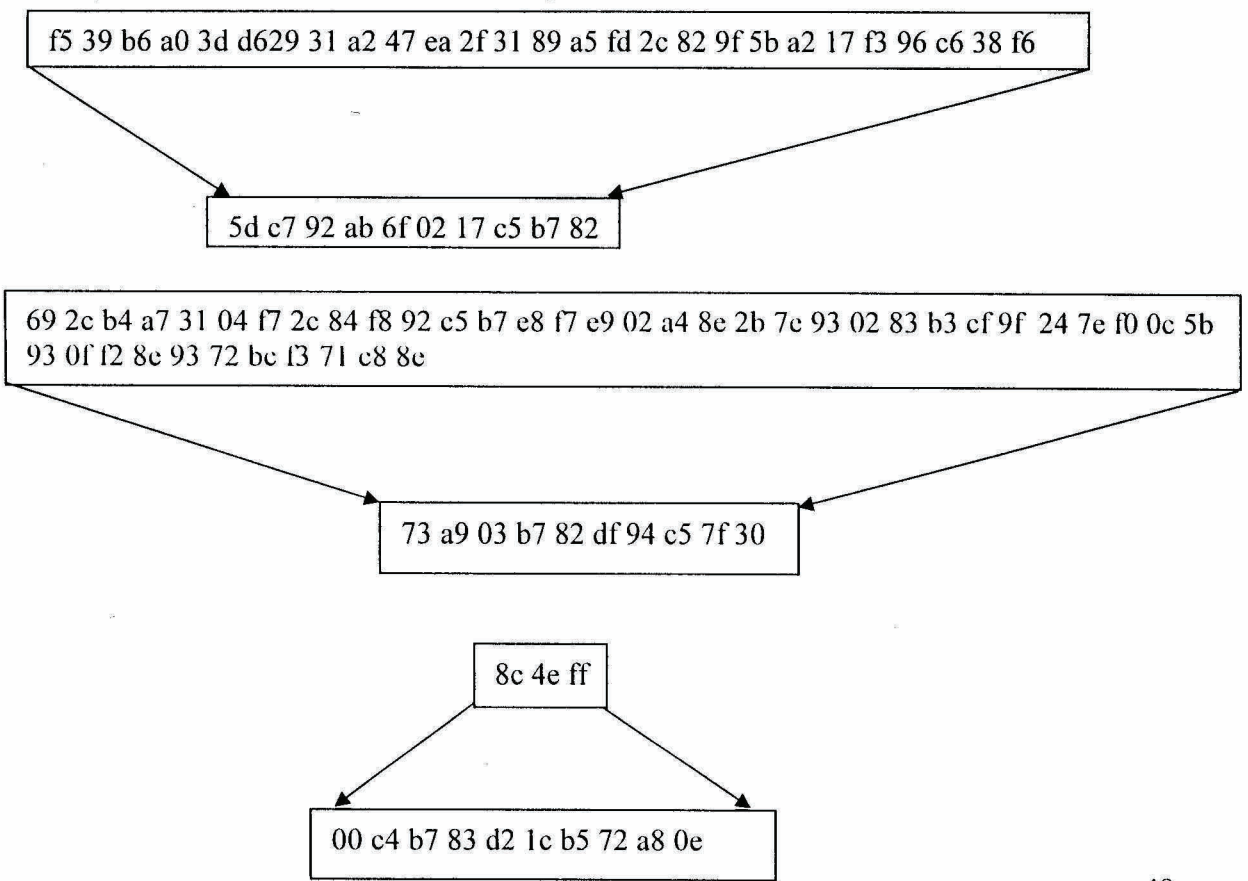
momento después de que un sistema criptografico es publicado y se muestra inmune a estos dos tipos de ataques (y algunos otros más) la mayor preocupación es la longitud de las claves.

7.1.2 Funciones Hash.

Una herramienta fundamental en la criptografía son las funciones hash, son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar pueden ser en general demasiado grandes la función hash les asocia una cadena de longitud 160 bits que son mas manejables para el propósito de firma digital.

De forma gráfica la función hash efectúa lo siguiente:



Esto es, un mensaje de longitud arbitraria lo transforma de forma "única" a un mensaje de longitud constante.

¿Cómo hace esto?

La idea general es la siguiente.

La función hash toma como entrada una cadena de longitud arbitraria, digamos 5259 bits, luego divide este mensaje en pedazos iguales, digamos de 160bits, como en este caso y en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de pedazos de 160 bits al último se le agrega un relleno, digamos de puros ceros. En nuestro caso en 5259 caben 32 pedazos de 160 bits y sobran 139, entonces se agregaran 21 ceros más.

7.2 Criptografía Asimétrica.

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas, proponen una forma para hacer esto, sin embargo no fue hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978, cuándo toma forma la criptografía asimétrica, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

La Criptografía asimétrica es muy usada, sus dos principales aplicaciones son precisamente el intercambio de claves privadas y la firma digital, una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario.

La criptografía asimétrica o de clave pública se divide en tres familias, Según el problema matemático del cual basan su seguridad.

La primera familia la que basa su seguridad en el Problema de Factorización Entera PFE, los sistemas que pertenecen a esta familia son, el sistema RSA, y el de Rabin Williams RW.

La segunda familia es la que basa su seguridad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de claves y el sistema DSA de firma digital.

La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etc.

7.2.1 RSA.

En el caso de RSA el problema matemático es el de la factorización de un número entero n grande (1024 bits), este número entero se sabe es producto de dos números primos p,q de la misma longitud, entonces la clave pública es el número n y la privada es p,q. El razonamiento del funcionamiento de RSA es el siguiente:

a) A cada usuario se le asigna un número entero n, que funciona como su clave pública.
b) Solo el usuario respectivo conoce la factorización de n (o sea p,q), que mantiene en secreto y es la clave privada.
c) Existe un directorio de claves públicas.
d) Si alguien quiere mandar un mensaje m a algún usuario entonces elige su clave pública n y con información adicional también pública puede mandar el mensaje cifrado c, que solo podrá descifrar el usuario correspondiente, el mensaje m convertido a número (codificación) se somete a la siguiente operación $c = n^e \bmod n$.

e) Entonces el mensaje c puede viajar sin problema por cualquier canal inseguro.

f) Cuando la información cifrada llega a su destino el receptor procede a descifrar el mensaje con la siguiente fórmula $m = c^d \bmod n$.

g) Se puede mostrar que estas formulas son inversas y por lo tanto dan el resultado deseado, (m,e) son públicos y se pueden considerar como la clave pública, la clave privada es la pareja (p,q) o equivalentemente el número d. La relación que existe entre d y e es que uno es el inverso multiplicativo del otro módulo $\lambda(n)$ donde $\lambda(n)$ es el mínimo común múltiplo de p-1 y q-1, esto significa que la clave privada o el de la pareja p,q o es el número d.

7.2.2 CCE

CCE otro tipo de criptografía de clave pública es el que usa curvas elípticas definidas en un campo finito. La diferencia que existe entre este sistema y RSA es el problema del cual basan su seguridad, mientras RSA razona de la siguiente manera: te doy el número 15 y te reta a encontrar los factores primos. El problema del cual están basados los sistemas que usan curvas elípticas que denotaremos como CCE es el problema del logaritmo discreto elíptico, en este caso su razonamiento con números sería algo como: te doy el número 15 y el 3 y te reta a encontrar cuantas veces tienes que sumar el mismo 3 para obtener 15.

Ventajas que ofrecen los CCE en comparación con RSA, la principal es la longitud de la clave secreta. Se puede mostrar que mientras en RSA se tiene que usar una clave de 1024 para ofrecer una considerable seguridad, los CCE solo usan 163 bits para ofrecer la misma seguridad, así también las claves RSA de 2048 son equivalentes en seguridad a 210 de CCE.

Los CCE son idóneos para ser implementados en donde el poder de computo y el espacio del circuito sea reducido, donde sea requerida una alta velocidad de procesamiento o grandes volúmenes de transacciones, donde el espacio de almacenamiento, la memoria o el ancho de banda sea limitado. Lo que permite su uso en Smart Cards, Teléfonos celulares, Fax, Organizadores de Palma, computadoras, etc.

VIII Software de control

8.1 Autenticación kerberos.

8.1.1 Introducción.

Kerberos es un sistema de control de accesos y autenticación completo inventado por el M.I.T. Las primeras versiones se realizaron para el sistema operativo UNIX.

Sus objetivos son:

- Exigir autenticación a los usuarios para la utilización del sistema y en particular para cada servicio ofrecido.
- Exigir autenticación a los servicios (software de los servidores).

Este sistema identifica usuario y servidor como objetos, por lo tanto, es independiente de las computadoras y su ubicación física. Es muy eficiente para conexiones remotas a servicios de uso restringido y permite centralizar la gestión de accesos.

8.1.2 Características.

- Utiliza únicamente clave simétrica
- Los passwords nunca viajan por la red.
- Se utiliza control de accesos individualizado para cada servicio, pero solo se introduce el password una vez por sesión.
- Se puede separar la red en diferentes dominios físicos de seguridad.
- Basa el control de accesos en un sistema (hardware y software), llamado Servidor de Autentificación AS, diferente de los servidores de información.

- En la versión 4 utiliza el algoritmo DES, en la 5 permite cualquier algoritmo y cualquier longitud de clave.

8.1.3 Funcionamiento.

Intervienen los siguientes elementos:

- Usuario.
- Servidor de servicios.
- Servidor de autentificación (AS).
- Servidor de concesión de tickets (TGS).

Aunque estos dos últimos pueden estar físicamente en la misma computadora.

Para que los passwords no viajen por la red se utilizan tickets para validar el acceso a los servicios. Estos tickets deben estar en posesión del usuario y enviarse a los servidores para conseguir el acceso. Un ticket es información encriptada con un passwords del sistema que permite el acceso al usuario que lo posee. Siempre tienen una fecha de caducidad para que no puedan ser aprovechados por los espías de la red. Tampoco se guardan passwords ni tickets en las computadoras de los usuarios para evitar a los Hackers que tienen accesos a estas computadoras.
El proceso de autenticación se divide en dos fases y 6 mensajes. En la siguiente figura se muestra estas fases.

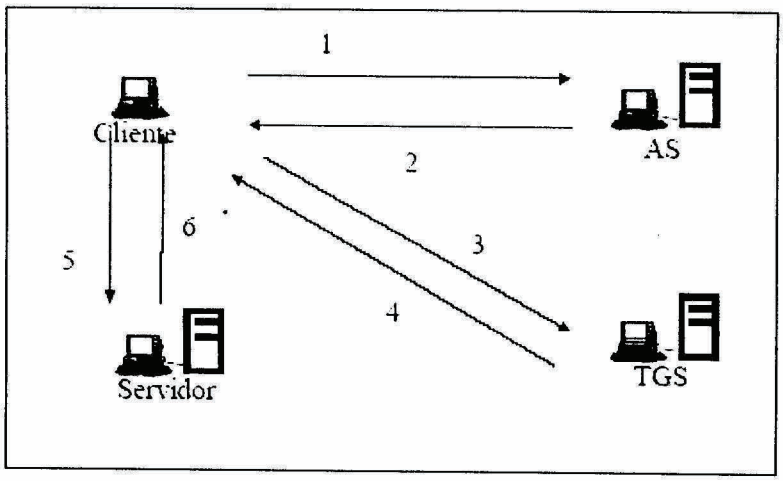


Figura proceso de autenticación Kerberos

Las fases son las siguientes:

1. Autenticación de usuario. Mensajes 1 y 2.
2. Autenticación de servicios. Mensajes 3, 4, 5 y 6.

Al conectarse se debe realizar la autenticación del usuario al sistema Kerberos y después se puede hacer tantas de servicios como se necesiten conectar, pero sin necesidad de repetir la de usuario.

8.1.4 Autenticación de usuario.

Se certifica el usuario al sistema, es la única fase del proceso donde se introduce el password. Esta autenticación sirve para posteriormente acceder al TGS, que concede tickets para los servicios.

El resultado final es la posesión del $TICKET_{TGS}$. Con este ticket se puede pedir autorización en el TGS a tantos servicios como se necesite.

La seguridad se basa en siguientes claves simétricas:

- El password del usuario genera (con un proceso matemático) una clave encriptar el mensaje 1. El AS posee la misma clave y con ella comprueba la autenticidad del usuario.
- El $TICKET_{TGS}$ esta encriptado como una clave conocida solamente por el TGS y el AS. Por lo tanto, el usuario no puede generar ni modificar un ticket de este tipo.
- Una clave se sesión generada aleatoriamente para las transmisiones entre TGS dentro del $TICKET_{TGS}$. Ninguna de las partes la puede modificar.

El resultado final es el ticket para el usuario, que no puede modificar y tiene una fecha de caducidad, y posteriormente el TGS lo reconocerá como autentico. También se recibe la clave de sesión a utilizar con el TGS. Si alguien captura el ticket en la línea no lo puede utilizar con el TGS ya que no conoce su clave de sesión, esta viene para el usuario encriptada con el password.

Al acabar esta fase se destruye el password de usuario. El $TICKET_{TGS}$ se puede utilizar para pedir autorización a varios servicios mientras no caduque, sin necesidad de volver a acceder al AS ni introducir el password.

8.1.5 Autenticación de servicios.

El usuario pide al TGS el $TICKET_{servicio\ x}$ para autenticarse delante del servicio X, también para comprobar la identidad de este. Este proceso se realiza tantas veces como servicios distintos quiera utilizar el usuario, pero nunca vuelve a introducir el password.

La seguridad se basa en siguientes claves simétricas:

- La clave de sesión
- El $TICKET_{SERVICIO\ x}$ esta encriptado con una clave conocida por el servicio X y el TGS.

- Una clave de sesión para utilizar en las comunicaciones entre el servicio y el usuario lo conoce el usuario porque llega encriptada con las clave de sesión actual y el servicio porque esta en el ticket. Ninguna de las partes la puede modificar.

El resultado es la obtención del $TICKET_{SERVICIO\ X}$ y una clave para la sesión con el servicio. Si alguien captura el ticket en la línea no lo puede utilizar ya que desconoce la clave se sesión.

El servicio se identifica utilizando la clave se sesión. Si es falso no podrá desencriptar el ticket y, por lo tanto, no tendrá la clave se sesión.

8.1.6 Instalación de Kerberos.

El software se puede conseguir gratis por Internet. Estas versiones no disponen de servicios técnicos, actualizaciones, instalaciones, ni formación por lo tanto, solo es aconsejable para pequeñas empresas. Existen muchas versiones comerciales de Kerberos con soporte técnico y formación a precios muy razonables.

A parte de comprar el software de cliente, el AS y el TGS se deben adaptar las aplicaciones cliente/servidor (los servicios) al entorno Kerberos. Esto puede suponer un aumento considerable de los costos de la instalación de este sistema y es muy importante tener en cuenta. Existen herramientas de programación para Kerberos, como GSS-API, útiles para adaptar el software y mantenerlo actualizado a los cambios en sistemas de autentificación.

Este sistema ofrece un entorno excelente para la seguridad de accesos y autenticación. Pero antes de instalarlo en una empresa se debe tener en cuenta los siguientes factores:

1. Debe formar parte de un plan de seguridad. Instalar Kerberos no supone resolver los problemas de seguridad. Un sistema Kerberos en una red sin seguridad es como un muro de papel con una puerta de acero.
2. Como mínimo necesita una computadora adicional para el AS y el TGS que este comunicada con todos los servicios y otra para Backup, porque la caída de la primera

significaría la denegación de todos los servicios de la red. Estas computadoras deben ser potentes ya que todos los accesos pasan por ellas.

3. La red debe ser rápida porque el sistema Kerberos genera muchos mensajes adicionales y se puede colapsar.
4. Supone gastos adicionales de personal para el mantenimiento del sistema.
5. Se debe adaptar a kerberos todo el software que presenta servicios con seguridad.
6. Asegurar la compatibilidad con los nuevos sistemas de autentificación. Si el sistema Kerberos es incompatible con otros servicios pronto se quedara aislado de la red Internet.
7. Necesita sincronización de todos los relojes de la red.

Por lo tanto, la instalación de Kerberos debe salir de un estudio muy cuidadoso del estado de la red y las necesidades de la empresa.

8.2 Autenticación Windows NT.

8.2.1 Esquema general.

Windows NT es un sistema operativo que utiliza autenticación de acceso a los objetos siguiendo una organización tipo DAC (Discretionary Access Controls). Así los propietarios de los objetos definen los permisos y derechos de los usuarios y grupos de usuarios.

Para iniciar el sistema operativo se necesita pasar un control de usuarios protegidos por contraseña y después para acceder a computadoras remotas también se examina la identidad del usuario. La organización de los accesos a computadoras de la red tiene un sistema de gestión único en Windows NT y este trabajo analiza este tipo de sistema.

El sistema de acceso a computadoras remotas se puede hacer según dos métodos diferentes, es así porque se intentan cumplir dos objetivos:

- La compatibilidad con sistemas anteriores de Microsoft, como: Windows 95, Windows 3.11 o DOS y sencillez para entornos con pocas computadoras.
- Crear un método de gestión centralizada donde las contraseñas no se deben actualizar en todas las computadoras de un mismo grupo de trabajo.

Así el acceso a recursos de red se puede instalar siguiendo uno de estos modelos:

- Trabajo en grupo. Este sistema implementa una red de igual a igual (peer to peer) que permite una gestión ágil para entornos con pocas computadoras, además de no necesitar la intervención de un Windows NT Server.
- Dominios. Un servidor centraliza todos los accesos a los servidores y clientes de su grupo llamado dominio.

8.2.2 Modelo de trajo en grupo.

Este modelo es mucho más difícil de gestionar y se debe utilizar en los siguientes casos:

- Redes pequeñas con pocas computadoras y pocos usuarios, donde la creación de dominios es mas complicada que la gestión de las bases de datos de usuarios.
- Redes donde computadoras con sistema operativo Windows deben compartir o acceder a recursos remotos.
- Redes Windows NT donde todos los sistemas operativos son Workstation y no hay Servers. Aunque se aconseja instalar Servers si la red es un poco grande.

Este modelo permite dos métodos de compartir recursos:

- Método compartido.
- Método de usuarios.

El método compartido su funcionamiento es el siguiente. El usuario local define los objetos que quiere compartir y les puede asignar una contraseña pero no un nombre de usuario. La

contraseña de un objeto compartido es la misma para todos los usuarios. Cuando se accede a un objeto protegido el servidor siempre pide una contraseña con independencia del usuario. Este sistema es muy poco seguro porque implica el reparto de contraseñas a todos los usuarios que pueden acceder.

Realizar la gestión del método compartido se complica mucho si hay varios recursos, sobre todo porque:

- Puede haber tantas contraseñas como recursos, por lo tanto, el usuario debe guardar la gestión de muchas contraseñas. Además se deben transmitir personalmente a cada usuario y esto comporta un gran peligro.
- Cualquier usuario puede dejar recursos de su computadora personal al acceso de cualquiera. Así la seguridad de la computadora esta en manos del usuario y no del gestor de red, por lo tanto puede haber múltiples agujeros y plataformas en la red sin que el gestor lo sepa.

El método de usuario necesita una computadora Windows NT o un servidor NetWare. Los accesos se realizan por nombre de usuario y contraseña. La base de datos de usuarios se guarda en una computadora NT o NetWare, el nombre de esta computadora se debe indicar en todas las que quieren compartir recursos utilizando esa base de datos. Para compartir recursos se asigna cada recurso a los usuarios de la base de datos.

Cuando se accede a un recurso de la computadora cliente envía los datos que el usuario introdujo para abrir la sesión en su computadora local, con estos datos se comprueba si puede acceder o no. Así no se debe dar la contraseña cada vez que se accede a un recurso.

Este método evita el tráfico de contraseñas del método compartido pero aunque mejora la gestión no se puede considerar un sistema centralizado. Presenta los siguientes problemas:

- Cualquier usuario puede dejar recursos de su computadora a disposición de quien quiera. Este permite tener computadoras no controladas que pueden ser agujeros o plataformas para otros ataques.

- Los usuarios se deben dar de alta en su computadora y en la base datos para los recursos. Si hay muchas bases de datos los cambios de contraseña se deben actualizar en todas.
- Solo se puede utilizar desde computadoras Windows NT donde la base de datos local tiene el mismo usuario que la remota. Por lo tanto o solo utilizan una computadora o se deben dar de alta en todas y así se pierde la ventaja de sistema centralizado.

8.2.3 Modelo de dominios.

Es el modelo de gestión centralizada ofrecido por Windows NT. Como mínimo debe haber un Windows NT Server para cada dominio.

La base de datos de usuarios se guarda en el controlador de dominios (PDC) y se duplica en los controladores secundarios (BDCs). Todos los controladores deben ser Windows NT Server. La duplicación se realiza para mantener el acceso si el PDC cae y para no concentrar todos los accesos en la misma computadora, frecuentemente los BDCs. Actualizan la base de datos, que pude ser únicamente los cambios o toda.

Los objetivos de los dominios son:

- Centralizar el control de accesos a las computadoras clientes. Así un usuario de un dominio se puede conectar a cualquiera de las computadoras de ese dominio, no hace falta que se de alta en la base de datos de todas.
- Gestionar el acceso a los recursos de manera ordenada. Desde la base de datos del dominio se pude acceder a los recursos de tu propio dominio sin necesidad de volver a ingresar la contraseña.

Cuando un usuario inicia una sesión en su computadora local puede introducir el nombre del dominio de esta computadora o entrar de forma local. Si entra por dominio, la computadora envía al controlador de dominio el nombre de usuario y la contraseña y el PDC realiza el control de accesos. Así el nivel de acceso a las computadoras locales y los servidores no depende de la base de datos local, es independiente de la computadora de acceso y, por lo

tanto, un sistema centralizado, siempre que la computadora de inicio de sesión este dentro del mismo dominio.

Dentro de una sesión de dominio, para acceder a un servidor del mismo dominio, la computadora local envía el nombre de usuario y la contraseña que el servidor comprueba en su base de datos. Si son servidores del dominio no PCD ni BDC pueden tener una base de datos de usuarios propios o utilizar la del dominio, pero nunca las dos. La contraseña solo se introduce al inicializar la sesión.

En resumen el sistema de dominios mejora respecto a los de trabajo en grupo:

- Se puede acceder al servidor desde cualquier computadora que pertenezca al dominio, no hay dependencia de la computadora de acceso.
- La base de datos local de acceso de las maquinas se puede centralizar en el controlador de dominio.
- El inicio de sesión dentro de un dominio asegura que se podrá acceder a los servidores del mismo dominio.

Los usuarios de un dominio se pueden conectar con servidores de otros dominios mediante las relaciones de confianza.

8.2.4 Relaciones de confianza entre dominios.

Las relaciones de confianza permiten a los usuarios de un dominio acceder a recursos de otros dominios. Se puede establecer relaciones unidireccionales (uno confía en el otro) o bidireccionales (confianza mutua). Otra solución seria dar de alta a los usuarios e todos los dominios que necesitan pero esto rompería el modelo de centralizacido ya que las contraseñas se deberían actualizar en varios controladores. Así con relaciones de confianza un usuario solo debe estar en una base de datos y puede acceder a varios dominios.

Se puede iniciar una sesión en un dominio de confianza. Si el controlador propio de la computadora ve que el domino es otro de confianza delega el control de acceso al controlador del dominio que ha pedido el usuario.

También se puede acceder a recursos de dominio de confianza. Cuando se accede a un servidor de otro dominio de confianza, este envía el nombre de usuario y la contraseña al controlador del dominio del usuario. Si el controlador admite el acceso, el servidor del dominio de confianza también.

Las relaciones de confianza son muy peligrosas porque los servidores no controlan directamente quien accede sino que delegan este control. Por este motivo se deben diseñar bien y gestionar de una manera centralizada. Microsoft recomienda utilizar una estructura jerárquica con un domino maestro en la cabeza que tiene relaciones de confianza unidireccionales con todos los dominios de trabajo.

8.2.5 Diferencias conceptuales con otros sistemas centralizados

El sistema de control de acceso Windows NT no es sistema completamente centralizado respecto a otros como los de directorios, como el NDS de Novell, o Kerberos.

Los objetivos del sistema de dominios son centralizar el control de acceso remoto y local mientras que los otros sistemas solo controlan el remoto. Así en Kerberos o directorios se debe realizar un control de acceso local (o acceso libre) y después otro remoto.

Las ventajas de cada sistema son:

- Windows NT solo utiliza un control de accesos para local y remoto.
- Los sistemas directorio y Kerberos permiten el acceso remoto desde cualquier computadora, no hace falta que sea del dominio.

Para solucionar este problema Windows NT ha creado las relaciones de confianza que permiten a computadoras de domino acceder a los otros. Pero son relaciones de bloque, o sea, o todos los usuarios o ninguno, no permiten casos personalizados.

Por el mismo motivo, los dominios de Windows deben crear una bese de datos de usuarios en cada grupo (servidor y sus clientes). En cambio los otros sistemas pueden centralizar la base de datos de usuarios en una computadora y, si fuera necesario para descargar transito, pueden dejar replicas totales o parciales en otras computadoras. En Windows NT esto se realizaría con un único dominio y muchos Vds. Pero entonces los usuarios podrían acceder localmente a cualquier computadora cliente.

IX Políticas de seguridad en red

9.1 Desarrollo de políticas de seguridad.

La primera regla de seguridad de una red es fácil: "Aquello que no esta permitido expresamente esta prohibido." Simple, una política de seguridad debe comenzar denegando acceso a todos los recursos de la red, y después dar acceso con una base especifica. Implementado de esta manera, la política de seguridad no permitirá ninguna acción o proceso inadvertido.

La meta en desarrollar una política oficial en seguridad de computadoras es definir las expectativas de la organización del uso correcto de la red y las computadoras y definir procedimientos para prevenir y responder a los incidentes de seguridad.

Para lograrlo, aspectos de la organización particular deben ser considerados y aceptados bajo el grupo creador de políticas.
La política de seguridad implementada debe ser conforme a otras políticas existentes, reglas, regulaciones, y leyes a las que la organización este sometida. Por ello será necesario identificarlas y tenerlas en consideración al desarrollar la política.

9.2 Aspectos a considerar para una política de seguridad.

Es importante considerar quien realizara la política de seguridad de la red. La creación de la política debe resultar del esfuerzo conjunto de un grupo representativo de gente que tome decisiones, personal técnico, y los usuarios del día a día de diferentes niveles en la organización. Los que toman decisiones (directivos) deben tener el poder de reforzar la política, el personal técnico aconsejara en las ramificaciones de la política, y los usuarios del día a día decidirán cuan utilizable la política. Un sistema con una política útil, inaplicable, o no desarrollable es inútil.

Desarrollar una política de seguridad compromete identificar los asientos organizacionales, identificar las amenazas, evaluar los riesgos, evaluar e implementar las herramientas y tecnologías disponibles para enfrentarse a estos riesgos, y desarrollar una política de uso. Además, un proceso de auditoria debe ser creado que revise el uso de la red y los servidores de una forma periódica. Además, una respuesta debe ser generada después de que una violación o delito ocurre.

Finalmente, la política debería ser comunicada a todo aquel que utilice la red de computadoras, empleado o subcontratado, y la política debe ser revisada de forma regular.

Es muy importante la formación a los usuarios para que se cumplan las políticas de seguridad, algo que prácticamente nunca se hace, lo que hace vulnerables muchas empresas a técnicas de hacking por ingeniería social, o simplemente encontrarse post-its con las claves de acceso pegados en el monitor de la gente (entre muchas otras cosas). Todo esto se podría evitar con una adecuada concienciación y formación al usuario.

9.3 Estrategias de seguridad.

El diseñar una estrategia de seguridad depende en general mucho de la actividad que se este desarrollando, sin embargo se pueden considerar los siguientes tres pasos generales: el primero crear una política global de seguridad, el segundo realizar un análisis de riesgos y el tercero aplicar las medidas correspondientes.

9.3.1 Política global de seguridad.

Se debe de establecer el estatus de la información para la empresa o la organización, debe de contener un objetivo general, la importancia de la tecnología de la información para la empresa, el periodo de tiempo de validez de la política, los recursos con que se cuenta, objetivos específicos de la empresa.

Debe de establecerse la calidad de la información que se maneja según su objetivo, la calidad que debe tener la información quiere decir que se establezca cuando o para quien la información debe ser confidencial, cuando debe verificarse su integridad y cuando debe de verificarse su autenticidad tanto de la información como de los usuarios.

9.3.2 Análisis de riesgos.

Consiste en enumerar todo tipo de riesgos a los cuales esta expuesta la información y cuales son las consecuencias, los posibles atacantes entre persona empresas y dependencias de inteligencia, las posibles amenazas etc., enumerar todo tipo de posible perdida desde perdidas directas como dinero, clientes, tiempo etc., así como indirectas: créditos, perdida de imagen, implicación en un litigio, perdida de confianza etc.

El riesgo se puede calcular por la formula riesgo = probabilidad × perdida, por ejemplo el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la perdida total en pesos de no hacer el contrato. El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la perdida en pesos de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña el riesgo es menor, pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la perdida total. Si por otro lado la pérdida es menor aunque la probabilidad de que ocurra el evento sea muy grande tenemos un riesgo menor. Por ejemplo la pérdida de una transacción de 300 pesos con una probabilidad muy grande de que ocurra al usar criptografía débil, el riesgo llega a ser menor.

En el análisis de riesgo debe también incluirse los posibles ataques que puedan existir y sus posibles efectos.

9.3.3 Medidas de seguridad.

Esta parte la podemos plantear como la terminación de toda la estructura de seguridad de la información. Una vez planteada una política de seguridad, decir cuanto vale la información, un análisis de riesgo, decir que tanto pierdo si le ocurre algo a mi información o que tanto se gana si se protege, debemos de establecer las medidas para que cumpliendo con la política de seguridad, las perdidas sean las menores posibles y que esto se transforme en ganancias ya sean materiales o de imagen.

X Auditoria informática

10 Estructura de los estándares para la práctica profesional de la auditoria de sistemas de información.

10.1 Introducción a las Normas Generales para Auditoria de Sistemas de Información.

Los sistemas basados en computadoras son herramientas útiles y omnipresentes que se aplican en la gestión y operación de muchas organizaciones. Tales sistemas pueden efectuar el control sobre muchos activos y operaciones de una organización. El desarrollo y respaldo de estos sistemas puede exigir una porción significativa de todos los recursos de la organización. Cuando se presentan tales condiciones, la misión del auditor puede incluir auditar el desarrollo, implementación, mantenimiento y operación de los sistemas.

El trabajo de los auditores, sean externos o internos, se rigen en general por estándares desarrollados por una cantidad de organizaciones profesionales, cada una de las cuales busca asegurarse de la calidad del trabajo de auditoria que se realiza.

10.2 Necesidad de Normas de Auditoria de Sistemas de Información.

El carácter especializado de la auditoria de sistemas de información y las habilidades necesarias para llevar a cabo una auditoria de esta índole requieren normas generales especificamente aplicables a la auditoria de sistemas de información. Como consecuencia de ello, uno de los objetivos de ISACA es proponer normas para satisfacer esta necesidad. El desarrollo y la difusión de las Normas de Auditoria de Sistemas de Información forman un móvil para la contribución profesional de ISACA a la comunidad de auditores.

10.3 Definición de la Auditoria de Sistemas de Información.

A los efectos de estas normas, la auditoria de sistemas de información se define como cualquier auditoria que cubre la revisión y evaluación de todos los aspectos (o alguna parte) de sistemas de procesamiento automatizado de información, incluyendo los procesos relacionados no automatizados, y las interfaces con ellos.
Los auditores de sistemas de información examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados (o tales sistemas como un todo) y sus interfaces con áreas no automatizadas de las operaciones de la organización. Los objetivos de tales auditorias por lo general son evaluar el grado en que estos sistemas o componentes de los mismos producen información confiable y exacta y determinar si tal información está en conformidad con requerimientos de la gerencia y cualquier disposición normativa aplicable.

10.4 Objetivos.

Los objetivos de las Normas de Auditoria de Sistemas de Información de ISACA son informar a:

Los auditores de sistemas de información del nivel mínimo de rendimiento aceptable que se requiere para cumplir con las responsabilidades profesionales expuestas en el Código de Ética Profesional para auditores de sistemas de información.

La gerencia y otras partes interesadas de las expectativas de los profesionales respecto de su propio trabajo.

El objetivo de las Directivas de Auditoria de Sistemas de Información es proporcionar información adicional sobre la manera de cumplir con las Normas de Auditoria de Sistemas de Información.

10.5 Alcance y Autoridad de las Normas de Auditoria de Sistemas de Información.

La estructura de las Normas de Auditoria de Sistemas de Información emitidas por ISACA establece múltiples niveles de estándares, como se indica a continuación:

Normas: definen los requisitos obligatorios para la auditoria de sistemas de información y la presentación de informes.

Directivas: brindan una orientación para la correcta aplicación de las normas de auditoria de SI. El Auditor de SI debe tenerlos en cuenta al determinar cómo llevar a cabo la implementación de las normas mencionadas, utilizar el juicio profesional en su aplicación y estar preparado para justificar cualquier desviación respecto de los mismos.

Procedimientos: brindan ejemplos de procedimientos que podría seguir un auditor de sistemas de información en un contrato de auditoria. Los documentos contienen procedimientos que proporcionan información sobre la manera de cumplir con las normas al realizar tareas de auditoria de sistemas de información, pero no establecen requisitos.

El Código de Ética Profesional de ISACA exige que los miembros de la Asociación y los titulares de la designación CISA (Auditor Certificado de Sistemas de Información) cumplan con las Normas de Auditoria de Sistemas de Información adoptadas por ISACA.
El manifiesto incumplimiento de las mismas puede conducir a una investigación de la conducta del miembro de la Asociación o del titular de la designación CISA por parte del Consejo Directivo de ISACA o del comité de ISACA que corresponda, con la eventual ocurrencia de acciones disciplinarias.

10.6 Relación entre las Normas de Auditoria de Sistemas de Información y otras Normas de Auditoria.

No se pretende que las normas de auditoria de sistemas de información promulgadas por ISACA reemplacen las normas de auditoria o reglamentaciones desarrolladas por otras organizaciones profesionales o entes gubernamentales. En situaciones en las que se perciba un conflicto entre las normas de ISACA y los de otro ente, es responsabilidad del auditor utilizar su juicio profesional, a partir de los hechos específicos de la situación, a fin de resolver la cuestión.

10.7 Código de ética profesional.

La Asociación fija el siguiente Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la Information Systems Audit and Control Association y poseedores del Certificado en Auditoria de Sistemas de Información.

Los Auditores de Sistemas de Información están comprometidos a sostener las siguientes prácticas:

- Apoyar el establecimiento y cumplimiento de normas, procedimientos, controles y procesos de auditoria de Sistemas de Información.
- Cumplir las Normas de Auditoria de Sistemas de Información adoptados por la Asociación.
- Actuar en interés de sus empleadores, accionistas, clientes y del público en general en forma diligente, leal y honesta y no a sabiendas de ser parte de actividades impropias o ilícitas.
- Mantener la confidencialidad de la información obtenida en el curso de las actividades asignadas. La información no será utilizada para beneficio propio o divulgada a terceros no legitimados.
- Cumplir con sus deberes en forma independiente y objetiva, y evitar toda actividad que comprometa, o parezca comprometer su independencia.

- Mantener su competencia en los campos interrelacionados de la auditoria y los sistemas de información por medio de su participación en actividades de desarrollo profesional.
- Poner sumo cuidado al obtener y documentar suficiente material provisto por el cliente que su consistencia servirá para basar sus conclusiones y recomendaciones.
- Informar a las partes involucradas acerca de los resultados de las tareas de auditoria llevadas a cabo.
- Apoyar la educación de la gerencia, los clientes, sus colegas y al público en general para mejorar la comprensión en materia de auditoria y de sistemas de información.
- Mantener altos los estándares de conducta y carácter tanto en las actividades profesionales como en las privadas.

10.8 Normas generales de auditoria de información.

Emitidas por el Comité de Normas de la Information Systems Audit and Control Association (ISACA)

010 Mandato de Auditoria

010.010 Responsabilidad, Autoridad y Rendición de Cuentas

La responsabilidad, autoridad y rendición de cuentas de la función de auditoria de sistemas de información deben ser adecuadamente documentadas en un estatuto de auditoria o términos de referencia de contratación.

020 Independencia

020.010 Independencia Profesional

En todos los asuntos relacionados con la auditoria, el auditor de sistemas de información debe ser independiente del auditado en actitud y apariencia.

020.020 Relación dentro de la Organización

La función de auditoria de sistemas de información debe ser lo suficientemente independiente del área auditada como para permitir la realización objetiva de la auditoria.

030 Ética y Normas Profesionales
030.010 Código de Ética Profesional

El auditor de sistemas de información debe observar el Código de Ética Profesional de ISACA (Information Systems Audit and Control Association).

030.020 Debido Cuidado Profesional

Se debe proceder con el debido cuidado profesional y deben observarse las normas aplicables de auditoria profesional en todos los aspectos del trabajo del auditor de sistemas de información.

040 Competencia
040.010 Habilidades y Conocimiento

El auditor de sistemas de información debe ser técnicamente competente y contar con las habilidades y el conocimiento necesarios para llevar a cabo sus tareas.

040.020 Capacitación Profesional Permanente

El auditor de sistemas de información debe mantener su competencia técnica por medio de una continua y adecuada capacitación profesional.

050 Planificación

050.010 Planificación de la Auditoria

El auditor de sistemas de información debe planificar las tareas de auditoria de tal manera que se aborden los objetivos pertinentes y se cumpla con las normas aplicables de auditoria profesional.

060 Realización de las Tareas de Auditoria

060.010 Supervisión

El personal de auditoria de sistemas de información debe ser adecuadamente supervisado a fin de garantizar que se alcancen los objetivos de auditoria y se cumpla con las normas aplicables de auditoria profesional.

060.020 Evidencia

En el transcurso de la auditoria, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoria con eficacia. Los hallazgos y las conclusiones de la auditoria deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia.

070 Presentación de Informes

070.010 Contenido y Estructura de Informes

El auditor de sistemas de información debe proporcionar a los destinatarios correspondientes un informe – con una estructura apropiada – sobre la realización de las tareas de auditoria. En dicho informe deben constar el campo de aplicación, los objetivos, el período de aplicación y la naturaleza y alcance de las tareas de auditoria realizadas.

El informe debe identificar la organización, los destinatarios correspondientes y cualquier restricción a su difusión; asimismo, debe exponer los hallazgos, las conclusiones y

recomendaciones y cualquier reserva o restricción que tenga el auditor con respecto a la auditoria.

080 Actividades de Seguimiento
080.010 Seguimiento

El auditor de sistemas de información debe solicitar y evaluar la información apropiada sobre anteriores hallazgos, conclusiones y recomendaciones pertinentes para determinar si se han implementado las medidas adecuadas de manera oportuna.

Fecha de Vigencia

Estas normas rigen para todas las auditorias de sistemas de información a partir del 25 de julio de 1997.

XI Marco jurídico de protección de datos

11.1 Introducción.

Las Tecnologías de Información y Comunicación (TIC), han revolucionado todos los ámbitos de la existencia humana.

Es ahí donde el Derecho, como regulador de las conductas del hombre en sociedad, debe intervenir de manera expedita y eficaz para evitar que la estampida de fenómenos informáticos que nos invade, escapen de control legal.

México está constituido como una República federal, en la que los Estados que la integran son libres y soberanos en cuanto a su régimen interior, si bien unidos por el pacto federal, por ello, los asuntos informáticos que inciden en el ámbito del Derecho Civil o Penal, pueden ser regulados por cada una de las Entidades Federativas a su libre y mejor parecer.

11.2 Delitos Informáticos.

Los delitos informáticos se define como. Aquellas conductas antisociales sancionadas por las leyes penales. Donde los quipos de cómputo son los objetivos del delito y cuyo resultado se encuentre sancionado por las leyes penales.

11.2.1 Ámbito federal.

- Modificación, destrucción o pérdida de información contenida en sistemas o equipos informáticos, (virus, gusanos).
- Conocer o copiar la información contenida en sistemas o equipos.
- Uso y/o reproducción no autorizada de programas informáticos con fines de lucro (piratería).
- Ataque a las vías de comunicación y obtención de información que pasa por el medio.
- Pornografía infantil.
- Asociación delictuosa y pandilla.

11.2.2 Ámbito local.

- Fraude (sistema financiero y administradores de negocio).
- Pornografía infantil delito informático.

11.3 Contratos Electrónicos.

La Ley de Instituciones de crédito y la Ley del Mercado de Valores, regulan el uso de medios electrónicos para la realización de sus operaciones.

El Código de Comercio, a partir del 2000 y con mayor precisión a partir del 2003, reconoce expresamente la contratación electrónica, regulando la creación de entidades certificadoras para asegurar la autenticidad de mensajes de datos y firma electrónica.

La ley Federal de Protección al Consumidor protege como confidencial la información que se proporciona al proveedor y obliga a éste a dar teléfono y domicilio físico.

El Código de Civil Federal y algunos Estatales, regulan como consentimiento expreso el manifestado por medios electrónicos y equiparan la oferta hecha entre presentes a la realizada por estos medios.

11.4 Protección de la privacidad y de la información.

Ley Federal de Protección al Consumidor.
Ley Federal del Derecho de Autor.
Ley de Instituciones de Crédito.
Iniciativa de Ley Federal de Protección de Datos Personales.
Ley de Protección de Datos Personales del Estado de Colima.
SPAM.

11.5 Propiedad Intelectual.

La Ley Federal del Derecho de Autor protege los programas de cómputo tanto operativos como aplicativos, excepto los que tengan efectos nocivos; también protege las bases de datos que por su composición constituyan obra intelectual.

11.6 Computo Forense.

Tanto el Código de Comercio, como la Ley de Instituciones de Crédito, la Ley del Mercado de Valores y el Código Federal de Procedimientos Civiles, le otorgan valor probatorio a los documentos o instrumentos que se obtengan por medios electrónicos.

11.7 Contenidos de Internet.

Prácticamente sin regulación, con la excepción de la pornografía infantil.

11.8 Código Penal Federal.

Titulo Noveno.

Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

11.8.1 Capitulo I

Revelación de secretos.

Artículo 210

Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211

La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis

A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

11.8.2 Capitulo II

Acceso ilícito a sistemas y equipos de informática.

Artículo 211 bis 1

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

XII Anexo I

12 20 Consejos para el usuario de plataformas Windows.

12.1 10 Básicas para la Seguridad de tu plataforma Windows como usuario conectado a Internet.

1. Actualizar a la última Release (edición) de la última plataforma publicada del OS MS-Windows (XP Pro recomendado).
2. Parchear el sistema www.microsoft.com/security y suscribirse al boletín de seguridad de Microsoft - Envía un mail vacío a: securbas@microsoft.com y sigue los pasos. Estarás informado de las fallas de este.
3. Hacer Update del sistema www.windowsupdate.com Visitar ese link y bajarse las actualizaciones disponibles - Deshabilitar el sistema de Update automático.
4. Instalar un Firewall Profesional - Los "Pro" tienen la opción de configurar el filtrado de protocolos y puertos a gusto de cada uno, en cambio el común viene por Default - Zonealarm Pro / Serial: dk68s-vfgfv-wh0jt-wnm68g-kx0w00
5. Deshabilitar servicios inútiles o puertos abiertos desde Services - Desde Administración del sistema se deshabilita por ejemplo Netbios, Unpnp, Telnet www.microsoft.com/security.
6. Instalar Antivirus, actualizar, escanear y configurarlo que monitoree actividad maliciosa en background* (* En tiempo real y archivos que se ejecutan) y correos electrónicos. Recomendado Norton 2004 www.symantec.com.
7. Instalar Antitroyano, actualizar, escanear y configurarlo que monitoree en background*. Recomendado The Cleaner www.moosoft.com - *Ejecutar TCActive! - Suscribirse a Virusattack!.
8. Instalar P.G.P - Solo el Plugin del Outlook Express y Pgp key management. - Parchearlo luego: PGP & Patches - Con ello podrás encriptar y firmar correos electrónicos entre amigos, además de malearse y que ningún ISP te los lea.

9. Steganos 3 Release 7 - Plataforma de seguridad en español: Disco rígido protegido, borrado seguro, esteganografía, bloqueo de computadora, codificador/decodificador y administrador de contraseñas. / Key: 41-107-96-61-37
10. Norton System Works 2004 - Instalar, configurar y dar un service completo - One button ckeckup, Ejecutar Norton System Works apretar Begin Scan, abajo a la derecha de la pantalla Inicial del programa. Al finalizar : Begin Fix.

12.2 10 Básicas para la Seguridad de la Información en su Sistema como usuario conectado a Internet.

1. Correos electrónicos: No ejecutar archivos atacados y manejarse solo con correos electrónicos en texto plano, no HTML. No contestar correos electrónicos de desconocidos desde el Outlook ya que damos a conocer nuestra posición en el Internet través del IP.
2. No hablar de cosas personales ni dar dato alguno a desconocidos que aparecen por IRC, ICQ, Correos electrónicos, Webchat, Teléfono, en la calle. Si los das procúrate de que sea alguien de suma confianza y asegúrate de que la seguridad de su computadora este en buen estado. No aceptes archivos en IRC, ICQ, FTPs, URL, de nadie desconocido el Internet través del IP.
3. Instruir a la persona "de confianza" (Cuidado con el hack local mas que nada por empleados desleales o compañeros de trabajo) que le dejes la computadora a cargo: Hermanos, empleados, parientes y amigos, coméntale los riesgos poniéndolo al tanto de estas básicas para que nadie se aproveche de él en el Internet, más si recién comienza a navegar por el Internet.
4. Elegir buenas contraseñas de mas de 8 dígitos alfanuméricas, no usar por ejemplo el mismo login que el password o cosas como nombre de pila o comunes: 123456, " tu birthday " , 111222, "mascota", fecha de nacimiento, admin, tu nick.

5. Siempre instalar los programas en modo Custom y no Standar, elegir cada componente a instalar. No instalar pro-gramas con Spyware, por ejemplo Kazaa y generalmente todos "famosos" freeware Checa la computadora con Ad-aware.
6. Huir de esos sitios de hosting gratuitos que tienen mp3/hack/sexo/warez/crack/downloads todo en uno y mil pop ups. Lo mas probable es que bajes programas troyanizados, haya scripts malignos y archivos con viejos virus.
7. Cambia los passwords de tus casillas de correo electrónico y conexión cada semana, los de tus FTP cada mes no solo los administradores de tu ISP ven tus pass día a día, sino mucha gente externa, amigos de los administradores e intrusos varios. El programa Steganos tiene un agradable y útil administrador de passwords.
8. No entrar a los URLs que te recomiendan desconocidos, es muy fácil hacer un "Fake Web" de "downloads" o puede ser algún servidor con Sircam u otro Worm. Puede ser también un sitio hecho para que bajes algún trojano sin saber o una falsa Gate o portal para chequear tu mail de Hotmail o Yahoo, falso obviamente. En IRC manéjate con precaución como así en los distintos puntos de encuentro donde haya personas desconocidas y crean ser "hackers".
9. En el caso de que uses: Script CGI y servicios como SSH, Telnet, Ftp, IIS por ejemplo, actualízalos siempre a la ultima versión y configúralos debidamente. Anótate en sus sitios para que te avisen de sus fallas y ultima versión. Por otro lado no le digas a todo el mundo el sofware que usas, como ser los de Servers, antivirus, firewalls.
10. Aprende, infórmate y estate al día, la seguridad informática o la seguridad de la información se disipa cada minuto, constantemente se desarrolla nueva tecnología, metodología, software y acciones para vulnerarla, no subestimes nada porque nada es seguro 100% y siempre hay alguien que sabe más, que el que más sabe.

XIII Conclusiones

En la actualidad las empresas no le dan la importancia y el valor de la información almacenada en un medio magnético por lo cual en el presente trabajo de investigación trato de explicar algunos de los aspectos que pudieran ser vulnerables a la información, por lo cual comento técnica y herramientas para reforzar la seguridad tanto física como lógica.

En la era digital en la que estamos viviendo, uno de los temas mas discutidos ha sido la seguridad en el flujo de información, diariamente nos encontramos con la necesidad de utilizar contraseñas para tener acceso a sistemas de información o incluso edificios y para llevar a cabo muchas de la de las tareas diarias, ya sea sacar dinero de un cajero automático, enviar un correo electrónico o navegar por Internet.

Una buena estrategia de seguridad es una herramienta necesaria para cualquier persona o empresa cuyas actividades impliquen el intercambio de información sensible a través de medios digitales de comunicaciones. Existen muy buenos productos de criptografía y herramientas forenses en el mercado, incluso algunos de ellos son gratis o pueden adquirirlos bajo licencias de sharewere. Sin embargo, existen también productos de muy mala calidad que no solo fallan en cuanto a sus promesas de seguridad, sino que también aportan argumentos negativos y confusión a lo que se refiere a seguridad en medios digitales.
La debilidad de los sistemas se encuentra en la inmensa capacidad de las supercomputadoras actuales, las cuales en cuestión de segundos pueden romper códigos complicados y en la perseverancia de la persona que ha decidido atacar sus comunicaciones.
Para saber que producto es el que le conviene más es necesario plantearse algunas preguntas por ejemplo: ¿necesita proteger todo un disco duro o solo algunos archivos? Es importante considerar el tipo de información que se envía y recibe si se trata de cadenas de correos electrónicos para los amigos o de información de sus cuentas bancarias, la importancia temporal de dicha información, si ya almacenada necesita estar a salvo de espías durante años o algunas horas y si esos espías son corporaciones, un ex empleado desguatado por su despido o simplemente un hacker que lo tome como un reto personal.

XIV Bibliografía

Libros

Milenkovic, Milan (1994). Sistemas Operativos: conceptos y diseño. 2ª Edición.

James L. Peterson, Abraham Silberschatz (1991). Sistemas Operativos, conceptos fundamentales.

Amparo Fuster Sabater, Dolores de la Guía Martínez, Luis Hernández Encinas, fausto Montoya Vitini, Jaime Muños Masque (2001). Técnicas Criptográficas de Protección de Datos 2ª Edición

Manuel Pons Martorell (2000). Control de Accesos

Maria Dolores Cerini, Pablo Ignacio (2002). Plan de Seguridad Informático.

V. Bátiz Álvarez, M. Farias Elinos (2003). Propiedad Intelectual y Protección de Datos

Soler Armando Donado, Miguel Ángel Niño Zambrano. Seguridad Computacional

Internet

http://www.isaca.org (Asociación de Auditoria y Control de Sistemas de Información)

http://www.securityportal.com.ar (Recopilación de Noticias de Seguridad)

http://www.hispasec.com (Seguridad y Tecnologías de la Información)

http://www.seguridad.unam.mx (Seguridad en Cómputo)

http://www.microsoft.com

http://www.delitosinformaticos.com

CD de diplomado "Informática Forense"