Universidad Nacional del Nordeste
Facultad de Ciencias Exactas, Naturales y Agrimensura

Informe de Adscripción

Seguridad en los Sistemas Operativos

Gabriela Mojsiejczuk - L.U.: 35.727

Prof. Director: Mgter. David Luis la Red Martínez

Licenciatura en Sistemas de Información
Corrientes - Argentina

Año 2007

Índice General

Índice de Figuras

Capítulo 1

Introducción

1.1 ¿Qué Es La Seguridad Informática?

Según la definición de la Real Academia de la Lengua RAE, *seguridad* es la cualidad de seguro, y *seguro* es algo libre y exento de todo peligro, daño o riesgo. Entonces se puede decir que la seguridad informática es un sistema informático exento de peligro.

Sin embargo se debe tener en cuenta que la seguridad no es un producto sino un proceso, por lo tanto se puede definir a la seguridad informática como: un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas [3, Neg95].

Día a día las listas de seguridad informática a nivel internacional publican una y otra vez las fallas más representativas de las aplicaciones y sus pruebas de concepto, reiterando que la *inseguridad* es una compañera permanente para los responsables de la seguridad informática en las organizaciones. En consecuencia, la seguridad total o 100% no es posible, pues no existe ningún elemento que no esté expuesto a situaciones no controladas o inesperadas, que alteren su funcionamiento, ya sea de manera positiva o negativa.

Algunas definiciones básicas que se deben tener en cuenta a la hora de hablar de seguridad informática se detallan a continuación.

1.1.1 ¿Qué Es Software Libre?

El término "Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software, y no al concepto de "gratis". De modo más preciso, se trata de cuatro libertades de los usuarios del software:

- La libertad de usar el programa, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa y adaptarlo a sus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias (libertad 2).
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie (libertad 3). El acceso al código fuente es necesario para esto.

La libertad para usar un programa significa la libertad para cualquier persona u organización de usarlo en cualquier tipo de sistema informático, para cualquier clase de trabajo, y sin tener obligación de comunicárselo al desarrollador o a alguna otra entidad específica.

También se debe tener la libertad de estudiar sus funciones, hacer modificaciones y utilizarlas de manera privada en el trabajo u ocio, sin ni siquiera tener que anunciar que dichas modificaciones existen.

La libertad de distribuir copias debe incluir tanto las formas binarias o ejecutables del programa como su código fuente, sean versiones modificadas o sin modificar.

Para que las libertades de hacer modificaciones y de publicar versiones mejoradas tengan sentido, se debe tener acceso al código fuente del programa. Por lo tanto, la posibilidad de acceder al código fuente es una condición necesaria para el software libre.

Son aceptables, sin embargo, ciertos tipos de reglas sobre la manera de distribuir software libre, mientras no entren en conflicto con las libertades centrales. Por ejemplo, copyleft ["izquierdo de copia"] es la regla que implica que, cuando se redistribuye el programa, no se pueden agregar restricciones

para denegar a otras personas las libertades centrales. Esta regla no entra en conflicto con las libertades centrales, sino que más bien las protege.

Un grupo de programadores ha comenzado a usar el término "open source" [código abierto] para designar algo parecido pero no idéntico a "free software" [Software Libre].

- La Licencia Pública GNU (General Public License) marca que todo software protegido por esta licencia debe poder ser redistribuido libremente, siempre que vaya acompañado por su código fuente, y debe poder ser modificado, embebido o reutilizado de cualquier manera, siempre que el resultado permanezca bajo la licencia GPL (Licencia Pública General).
- La Licencia Académica, creada por la Universidad de California en Berkeley para las modificaciones que se hicieron al código fuente original del Unix de AT&T, conocido como Berkeley Software Distribution.
- La Licencia BSD permite la redistribución de los programas que protege bajo cualquier esquema, siempre y cuando se otorgue crédito a los autores originales. El espíritu de esta licencia puede apreciarse claramente en las políticas de copia del sistema operativo OpenBSD.

1.2 ¿Qué Es Un Sistema Operativo?

Un Sistema Operativo es un conjunto de programas de proceso con las rutinas de control necesarias para mantener continuamente operativos dichos programas [2, LRMDL].

1.2.1 Principales Funciones Del Sistema Operativo

- Abstracción del hardware.
- Compartir los recursos justamente.
- Proteger a todos los procesos de los demás procesos.
- Proteger a los datos de todos los usuarios de los demás usuarios.
- Asegurar la integridad de la información.

1.2.2 Sistemas Operativos Libres y Sus Características Principales

Linux

- Es el sistema operativo libre más popular.
- Desarrollado completamente bajo un esquema cooperativo y no centralizado, lo que ha llevado a la aparición de muchas distribuciones.
- Bajo casi todas las distribuciones, su seguridad es bastante débil en la configuración por defecto (default).
- Muy alta velocidad de desarrollo e innovación.
- Soporte a una amplia gama de plataformas de hasrdware.

FreeBSD

- Su objetivo es crear un sistema operativo libre con la máxima estabilidad y eficiencia para plataformas Intel; recientemente agregó soporte para plataformas Alpha.
- Derivado de las fuentes originales de BSD, con una trayectoria de tres décadas de desarrollo.
- Es el sistema derivado de BSD más popular.
- Desarrollado abiertamente por un núcleo cerrado de desarrolladores, con contribución de los miembros de la comunidad.
- Alta velocidad de desarrollo e innovación.

OpenBSD

- Reconocido sin lugar a dudas como el sistema operativo más seguro del mundo.
- Derivado de NetBSD, el cual a su vez deriva de las fuentes originales de BSD, con una trayectoria de tres décadas de desarrollo.

- Desarrollado abiertamente por un núcleo cerrado de desarrolladores, con contribución de los miembros de la comunidad.
- Auditoría proactiva constante de seguridad en el código.
- Primer sistema operativo en integrar el soporte a la criptografía fuerte como característica núcleo del sistema.
- Da mucha mayor importancia a la seguridad y estabilidad que a adoptar nuevas características.
- Soporta una amplia gama de plataformas de hardware.

Sistemas Menores

- NetBSD: Su objetivo es ser un sistema operativo libre que soporte tantas arquitecturas de hardware como sea posible.
- AtheOS: Busca crear un sistema operativo para escritorio eficiente, fácil de utilizar y GPL (Licencia Pública General).
- HURD: Implementa un diseño avanzado de microkernel, se convertirá en el núcleo central del sistema GNU.
- FreeDOS: Reimplementación libre compatible con MS-DOS.
- MIT-Exokernel: Propone optimizar al sistema operativo para cada aplicación, logrando resultados sorprendentes.

1.3 ¿Qué Es Seguridad?

Seguridad es una palabra con una definición demasiado amplia, y aún entre expertos es difícil llegar a un acuerdo acerca de qué significa.

En el ámbito informático, la seguridad equivale principalmente a garantizar al usuario:

- *Consistencia:* Comportarse como se espera que se comporte y mantener su comportamiento sin cambios inesperados.

- *Servicio:* El sistema debe prestar todos los servicios que ofrece de manera confiable, constante y consistente.
- *Protección:* Si un programa tiene errores y sufre una caída, no debe afectar a la ejecución de otros procesos. Un programa diseñado expresamente para hacer daño debe tener un impacto mínimo en el sistema. Los segmentos de memoria de un proceso deben ser invisibles e inmodificables para cualquier otro proceso.
- *Control de Acceso:* Los datos generados por un usuario no deben ser accesibles a otro usuario a menos que así sea específicamente solicitado por su dueño. Soportar diferentes modos de acceso a un archivo, de modo que el sistema pueda exigir que un archivo pueda ser leído pero no ejecutado o abierto para escritura. Los mecanismos de control de acceso deben ser tan granulares como sea posible.
- *Autenticación:* El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es quien dice ser y tiene suficientes privilegios para llevar a cabo todas las operaciones que desee realizar. Debe ser capaz de notificar al administrador acerca de cualquier anomalía.

1.3.1 Imposibilidad De Lograr La Seguridad Absoluta

- Siempre habrá agujeros (fallas en la lógica de los programas) desconocidos para el responsable del sistema.
- Siempre habrá riesgos desconocidos para el programador de cada uno de los componentes del sistema.
- La seguridad es inversamente proporcional a la usabilidad.

1.4 ¿Qué Es Una Herramienta De Seguridad?

- Una herramienta de seguridad es un programa que corre en espacio de usuario diseñado para ayudar al administrador, sea alertándolo o realizando por sí mismo las acciones necesarias a mantener un sistema seguro. Pueden ser:
- *Orientadas a host:* Trabajan exclusivamente con la información disponible dentro del host (configuración, bitácoras, etc.).

- *Orientadas a red:* Trabajan exclusivamente con la información proveniente de la red (barridos de puertos, conexiones no autorizadas, etc.).

  Muy importante: Toda herramienta de seguridad útil para el administrador es también útil para un atacante, y toda herramienta de seguridad disponible para un administrador se debe asumir que está también disponible para un atacante.

1.5 Amenazas A La Seguridad

1.5.1 Identificación De Amenazas

A la hora de proteger los recursos del sistema es primordial identificar las vulnerabilidades y amenazas que ciernen contra ellos. Una *vulnerabilidad* es cualquier situación que pueda desembocar en un problema de seguridad, y una *amenaza* es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

- *Desastres del entorno:* Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

- *Amenazas en el sistema*: Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad.

- *Amenazas en la red:* Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante

redes locales, Intranets o la propia Internet, y esta interconexión acarrea nuevas y peligrosas amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que se conecta desde su casa a través de un módem).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar la seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en piratas informáticos llamados "hackers". No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre se debe de contemplar a las amenazas como actos intencionados contra el sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación. Por supuesto, tampoco es correcto pensar solo en los accesos no autorizados al sistema: un usuario de una máquinas puede intentar conseguir privilegios que no le correspondan, una persona exterña a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un login y una contraseña, etc.

Principales Amenazas De Seguridad Informadas Por McAfee Avert Labs Para El Año 2007

El 29 de diciembre de 2006 se publicaron las diez principales amenazas de seguridad informadas por McAfee Avert Labs para el año 2007, sin un orden en particular se listan a continuación:

1. Aumentará la cantidad de sitios Web para robar contraseñas mediante el uso de páginas de inicio falsas para servicios en línea populares como eBay.

2. El volumen del spam, en particular del spam con imágenes que consume gran ancho de banda, seguirá aumentando.

3. La popularidad del uso compartido del video en la Web hace inevitable que los hackers comiencen a usar archivos MPEG como un medio de distribuir código malicioso.

4. Los ataques a teléfonos móviles se harán más frecuentes a medida que los dispositivos móviles se hagan más "inteligentes" y con mayor conexión.

5. Los programas publicitarios fortalecerán su dominio siguiendo el aumento de los posibles programas no deseados (PUP, Potentially Unwanted Programs) comerciales.

6. Los robos de identidad y la pérdida de datos seguirán siendo un problema público: el origen de estos crímenes a menudo se encuentra en el robo de computadoras, la pérdida de respaldos y el compromiso de sistemas de información.

7. Se incrementará el uso de bots, programas computacionales que realizan tareas automatizadas, como una herramienta favorita para los hackers.

8. Reaparecerá el malware parasitario, o virus que modifican los archivos existentes en un disco.

9. Se registrará un aumento en la cantidad de rootkits en plataformas de 32 bits; sin embargo, las capacidades de protección y reparación también se potenciarán.

10. Las vulnerabilidades seguirán causando preocupaciones fomentadas por el mercado clandestino de las vulnerabilidades.

11. Motivaciones para implementar mecanismos de seguridad.

1.6 Conceptos Fundamentales Sobre La Seguridad Informática

1.6.1 Niveles De Seguridad

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Como no es posible la certeza absoluta, el elemento de riesgo siempre esta

Figura 1.1: Niveles de Seguridad

presente, independiente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. Se entiende como seguridad informática a un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, lo que requiere también un nivel organizativo, podemos decir que:

Sistema de Seguridad = TECNOLOGIA + ORGANIZACION

1.6.2 Las Técnicas De Respaldo y Los Sistemas Redundantes

Los sistemas de respaldo (backup) y los sistemas redundantes son dos técnicas para proteger los datos contra pérdida por borrado accidental o desastres fortuitos. Ambos sistemas son complementarios en cuanto a la seguridad que ofrecen ya que tanto los respaldos como la redundancia, por si solos, no cubren toda la necesidad.

Redundancia: los sistemas RAID.

Un *RAID* (Redundant Array Of Independent/Inexpensive Disks) es un conjunto de unidades de disco que aparecen lógicamente como si fueran un solo disco. Así los datos, distribuidos en bandas, se dividen entre dos o más unidades. Esta técnica incrementa el rendimiento y proporciona una redundancia que protege contra el fallo de uno de los discos de la formación. Existen

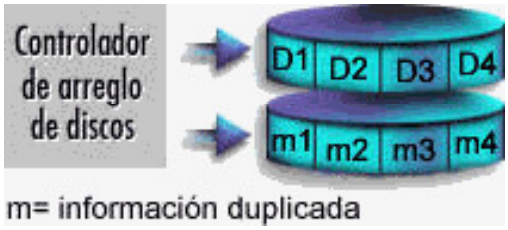

Figura 1.2: Nivel RAID 0

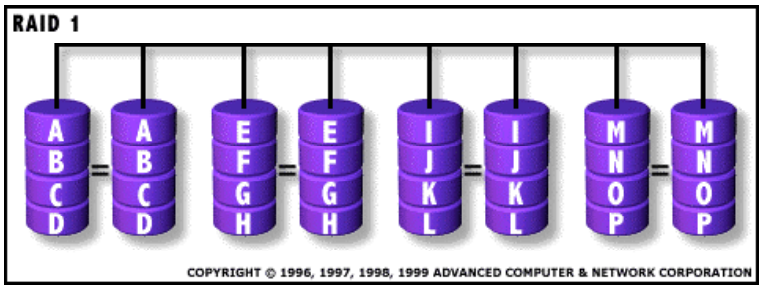

Figura 1.3: Nivel RAID 1

varios niveles RAID a partir del nivel 0, en el que los datos se dispersan en varias unidades pero no hay redundancia (gran rendimiento pero nula seguridad). Luego el nivel 1 o mirroring (espejo) en el cual los datos se escriben duplicados en distintas unidades, este método no incrementa el rendimiento pero si la seguridad y es, de hecho uno de los más utilizados. Los demás niveles RAID son una combinación de los conceptos anteriores y buscan aumentar la seguridad y el rendimiento simultáneamente.

Existen sistemas operativos, que ofrecen administración RAID incorporada, como por ejemplo Windows NT que ofrece los niveles 0, 1 y 5. Como es obvio si se implementa el nivel 1 (discos espejo, donde todo lo que se escribe en un disco es duplicado automáticamente), la duplicación debe ser en un disco físico diferente.

1.6.3 Tolerancia A Fallos

La *tolerancia a fallos* es la capacidad de un sistema a responder a un suceso inesperado, como puede ser un fallo de suministro eléctrico o un fallo de hardware de forma que no se pierdan datos. Cabe señalar que la redundancia no protege contra el borrado accidental, la operación negligente, etc. ya que cualquier operación (aún las erróneas) es automáticamente duplicada en todas las unidades. Así, la redundancia, junto con los sistemas de alimentación ininterrumpida (UPS y grupos electrógenos) proporcionan seguridad solamente en caso de cortes de suministro o fallos del hardware.

1.6.4 El "Backup"

El *"backup"* consiste en realizar copias de seguridad de la información. Estas copias pueden realizarse de forma manual y periódica. Pero, ¿Cual es el objeto de hacer copias manualmente si tenemos un sistema redundante?. La ventaja de los "backups" es que por efectuarse según ciertos períodos, la información respaldada no es exactamente igual a la actual. Esto permite cierta protección contra los errores humanos, borrado accidental o uso negligente ya que si no se detecta a tiempo, antes de que se cometa un "backup" del error, se pueden recuperar los datos con cierto desfase de tiempo y solo será necesario actualizar ese desfase.

Los sistemas de copia de seguridad más recomendables son los que dejan dos desfases: diarios y semanales por ejemplo.

1.6.5 Virus y Troyanos

También existen las amenazas de los virus y programas troyanos. Los mecanismos conocidos hasta el momento para la propagación de virus son los archivos ejecutables, es decir aquellos con extensión .exe, .com o .bat, y los componentes de Microsoft Office que aceptan macros con el lenguaje Visual Basic para Aplicaciones, principalmente Word y Excel con macros. Los troyanos se propagan también a través de archivos ejecutables. Así la única forma conocida en que un virus o troyano puede instalarse en un equipo es:

- Ejecutando un programa infectado, ya sea directamente desde un diskette, bajado desde Internet o abierto desde un "attach" recibido por

correo electrónico.

- Abriendo un documento de MS-Office 97 (o superior) teniendo deshabilitada o haciendo caso omiso a la alerta contra macro virus habilitada por defecto en Office.

Es decir que las precauciones elementales contra la adquisición de un virus o troyano son:

1. No usar programas grabados en diskette, particularmente juegos o utilidades de procedencia desconocida.
2. No usar programas bajados de sitios poco confiables de Internet.
3. No abrir attach de correo electrónico cuyo contenido o remitente se desconozcan o no sean de confianza.

Existe una gran variedad de virus cuyos efectos van desde los simplemente molestos hasta los que destruyen información específica o bien toda la contenida en el disco duro. Lo característico de los virus es que una vez que se instalan en el ordenador pasan largo tiempo sin provocar ningún efecto, aparte de infectar a todos los demás programas que se ejecuten.

1.6.6 Métodos De Protección Contra IntrusionesRemotas.

En su aspecto más básico, la protección contra "caballos de troya" se basa en el uso de antivirus que tienen la capacidad de detectar los troyanos más conocidos.

Sin embargo existe la posibilidad de ataques más sofisticados por lo que se hace necesario el uso de software del tipo cortafuegos "firewalls" o detectores de Intrusiones, que monitorizan los intentos de introducirse a un sistema sin la debida autorización como ataques a la Intranet.

Estos detectores pueden estar basados en los Host (Omni Guard, Stalker y otros) o en la red (Real Secure, Cyber Cop, Net Ranger). La detección de intrusos es bastante cara y constituye solo parte de un sistema completo de seguridad, que puede complementarse con sistemas de autentificación fuerte como Safeguard VPN.

Figura 1.4: Seguridad de la Información

Después de este período el virus actúa sobre el equipo en que esta instalado.

Los troyanos son programas que permiten a extraños intervenir en un ordenador remoto que está conectado a Internet, es lo que se conoce como "hackear" o más correctamente "nukear" un computador remoto. Existen una multitud de programas que permiten hacer esto como lo son netbus, mere, back oriffice, Backdoor.SubSeven.20, etc.

Pese a sus diferentes efectos, virus y troyanos comparten características comunes en su forma de operar y propagarse, pero cabe señalar que los antivirus actuales detectan indistintamente virus y troyanos.

1.7 Confidencialidad, Integridad y Disponibilidad De La Información

Lo importante es proteger la información. Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos), son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la *confidencialidad, la integridad y disponibilidad de la información.*

1.7.1 Confidencialidad

La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas", la intercepción o recepción electromagnética no autorizada, o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

1.7.2 Integridad

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

1.7.3 Disponibilidad

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

1.7.4 Otros Problemas Comunes

Otros problemas importantes de seguridad son la autentificación, es decir, que se garantice que quien firma un mensaje es realmente quien dice ser; el no repudio, es, que alguien niegue haber enviado una determinada información cuando efectivamente lo hizo, y los controles de acceso, esto es quien tiene autorización y quien no para acceder a determinada información.

Finalmente se tiene el problema de la verificación de la propiedad de la información, es decir que una vez que se ha detectado un fraude determinar la procedencia de la información.

1.7.5 Daños No Intencionados

No todos los riesgos que amenazan la información son de origen dañino. Es por eso que las medidas de seguridad no deben limitarse a la mera protección contra ataques e intrusiones de terceros, pues dentro de la misma organización y por parte de individuos de confianza existen riesgos contra la disponibilidad de la información ya sea por negligencia, descuido, ignorancia o cualquier otro tipo de mala práctica, la información puede ser alterada, sustituida o permanentemente borrada. Además están siempre presentes los riesgos de pérdida o alteración por virus o situaciones de fuerza mayor, tales como incendios, inundaciones o catástrofes naturales.

1.8 Amenazas y Métodos De Defensa

Esta sección describe una serie de amenazas de seguridad para la red identificadas por el modelo STRIDE (imitación, manipulación, rechazo, revelación de información, denegación de servicios, elevación de privilegios) y la manera en que las medidas de seguridad implementadas como parte de esta solución pueden utilizarse para reducirlas.

1.8.1 El Modelo De Identificación STRIDE

Amenazas de imitación de identidad

Las amenazas de imitación de identidad incluyen cualquier actividad orientada a obtener acceso y utilizar, ilegalmente, la información de autenticación de otra persona, como pueden ser el nombre de usuario o la contraseña. Esta categoría de amenaza incluye los ataques de intermediario y las comunicaciones de hosts de confianza con hosts que no son de confianza.

Ataques de intermediario

Una técnica común que utilizan los piratas informáticos es el ataque de intermediario. Esta técnica coloca un equipo entre dos equipos que se comunican en una conexión de red. Seguidamente, el equipo que está en medio suplanta a uno de los equipos originales o a ambos. Esta técnica proporciona al "intermediario" una conexión activa con los equipos originales y la capacidad de leer o modificar los mensajes conforme pasan entre ellos; mientras

tanto, los usuarios de los equipos originales no perciben anomalía alguna en la comunicación.

Algunos proveedores de servicios de Internet (ISP) han desarrollado prácticas de filtrado que intentan combatir tanto los ataques de intermediario como la imitación del correo electrónico. Por ejemplo, muchos ISP sólo autorizan que los usuarios envíen correo electrónico a través de los servidores del ISP y justifican esta restricción con la necesidad de combatir el correo electrónico no deseado. No obstante, de este modo también se impide a los usuarios autorizados que utilicen servicios legítimos de correo electrónico de terceros, lo que suele molestar a muchos usuarios avanzados. Algunos ISP de cable intentan bloquear el tráfico de audio o vídeo para obligar a los usuarios a utilizar sus propios servicios de voz sobre IP o de transmisión de vídeo.

Los filtros de los ISP se implementan normalmente mediante funciones de hardware de los enrutadores que funcionan sobre determinados tipos de protocolo (protocolo de datagrama de usuario, UDP, o protocolo de control de transmisión, TCP), números de puerto o indicadores TCP (paquetes de conexión inicial en lugar de datos o confirmación). El uso de IPsec deshabilita con eficacia este tipo de filtrado, dejando al ISP sólo con dos opciones muy drásticas: prohibir todo el tráfico IPsec o prohibir el tráfico con ciertos interlocutores identificados.

Comunicación de hosts de confianza con hosts que no son de confianza

Esta amenaza es realmente un superconjunto de varias amenazas menores e incluye los problemas relacionados con la imitación de identidad en general, la modificación de datos entre los extremos de una transmisión y la interceptación. Sin embargo, la amenaza más importante es la imitación porque el propósito es engañar a un host de confianza para que "crea" que se está comunicando con otro host de confianza.

No todos los hosts que se vayan a aislar precisan comunicarse con hosts que no son de confianza. Puesto que IPsec utiliza un mecanismo basado en directivas para determinar el nivel de seguridad que se requiere entre dos hosts cuando empieza la negociación, la mayoría de estos problemas se resuelven considerando cuidadosamente ventajas e inconvenientes de la seguridad y la comunicación y, a continuación, llevando a cabo procesos de diseño e implementación de una directiva IPsec bien pensados, que reflejen el resultado preferido.

Manipulación de datos

Las amenazas de manipulación de datos están relacionadas con la modificación malintencionada de los datos. Los ejemplos incluyen la realización de cambios de datos persistentes sin autorización (como la desfiguración de sitios Web), información contenida en una base de datos o la alteración de datos mientras circulan de un equipo a otro en una red abierta. Una amenaza específica de esta categoría es el secuestro de sesión.

Secuestro de sesión

Unos mecanismos de autenticación bien diseñados y unas contraseñas largas y aleatorias proporcionan resistencia ante el espionaje de redes y los ataques de diccionario, respectivamente. No obstante, los atacantes pueden utilizar el secuestro de sesión para capturar una sesión, una vez que el usuario legítimo ha sido autenticado y autorizado.

El secuestro de sesión puede habilitar a un atacante para que utilice los privilegios de un usuario habitual con el fin acceder a una base de datos o modificarla, quizá para instalar software que le permita penetrar más a fondo, incluso sin obtener las credenciales del usuario habitual.

La manera más sencilla de secuestrar una sesión consiste, primeramente, en intentar la colocación del equipo del atacante en algún lugar de la ruta de conexión utilizando una herramienta de piratería especializada. El atacante observará el intercambio y, en algún momento, entrará en acción. Puesto que el atacante se encuentra en medio del intercambio, es capaz de finalizar uno de los lados de la conexión TCP y mantener el otro lado utilizando los parámetros TCP/IP y números de secuencia correctos. El uso de IPsec para cifrado o autenticación protege los extremos contra el secuestro de sesión.

Rechazo

Las amenazas de rechazo están asociadas con usuarios que niegan haber ejecutado una acción, pero no existe forma alguna de probar lo contrario. Un ejemplo de este tipo de amenaza se produce cuando un usuario realiza una operación prohibida en un sistema que no tiene la capacidad de rastrear dicha operación. No rechazo se refiere a la capacidad que tiene un sistema de contrarrestar las amenazas de rechazo. Por ejemplo, un usuario que compra un artículo a un proveedor basado en Web tendrá que firmar en el momento en que lo reciba. El proveedor podrá usar este recibo firmado como prueba de que el usuario ha recibido el paquete.

Divulgación de información

Las amenazas de revelación de información están relacionadas con la divulgación de información entre individuos que no deberían tener acceso a la misma. Los ejemplos incluyen aquellos usuarios que pueden leer archivos a los que no se les ha concedido acceso o los intrusos que leen datos en tránsito entre dos equipos. Las amenazas de esta categoría incluyen las conexiones no autorizadas y el espionaje de redes.

Conexiones no autorizadas

Muchas configuraciones de red presentan una postura de seguridad muy confiada y conceden acceso a grandes cantidades de información desde los equipos del interior del perímetro. El acceso es a veces explícito (como es el caso de los servidores Web de Intranet) y otras implícito, debido a la escasa protección de algunas aplicaciones. Algunas directivas confían en simples comprobaciones de la dirección, pero los atacantes pueden eludir estas pruebas falsificando las direcciones.

Se puede utilizar IPsec para implementar una comprobación adicional de la conexión. Es posible establecer reglas de directiva que requieran que sólo se pueda acceder a un conjunto de aplicaciones una vez que la negociación IPsec haya concluido correctamente.

Espionaje de redes

Los atacantes intentan captar el tráfico de red por dos motivos: para obtener copias de archivos importantes durante su transmisión y lograr contraseñas que les permitan ampliar la penetración. En una red de difusión, los piratas informáticos utilizan herramientas de espionaje de redes para registrar las conexiones TCP y lograr copias de la información transmitida. Aunque estas herramientas no funcionan muy bien en redes conmutadas, incluso en este tipo de redes se puede atacar el protocolo de resolución de direcciones (ARP) mediante otras herramientas especializadas que redirigen el tráfico IP a través del equipo del atacante para facilitar el registro de todas las conexiones.

Algunos protocolos (protocolo de oficina de correo 3, POP3, y protocolo de transferencia de archivos, FTP, por ejemplo) continúan enviando contraseñas de texto sin formato por la red, con lo que no le resultará muy difícil a un atacante obtener esta información. Muchas aplicaciones utilizan un mecanismo de desafío/respuesta que evita el problema del envío de contraseñas de texto sin formato, pero el desafío presentado sólo es ligeramente más complejo. El

atacante no puede leer la contraseña directamente, pero los ataques de diccionario permiten deducirla a partir de una copia del desafío y la respuesta. El uso de IPsec para cifrar este tipo de intercambios protege con eficacia contra el espionaje de redes.

Denegación del servicio

Los ataques de denegación de servicio son ataques dirigidos contra un host o una red específica. Normalmente, estos ataques suelen enviar más tráfico a un host o enrutador del que puede gestionar en un tiempo determinado. Ello da como resultado la incapacidad de la red de gestionar el tráfico, por lo que el flujo legítimo de éste se ve interrumpido.

Los ataques de denegación de servicio pueden estar distribuidos entre muchos atacantes que centran el esfuerzo en un objetivo en particular. Los equipos objeto de estos ataques suelen quedar expuestos a algún peligro. Se instala en ellos una secuencia de comandos o un programa malintencionado que permitirá al atacante utilizar los equipos para dirigir una avalancha de tráfico de red que pretende desbordar otro equipo o grupo de equipos. Los equipos comprometidos se denominan zombies, y este tipo de ataque se conoce como ataque de denegación de servicio distribuido.

IPsec requiere autenticarse antes de establecer la comunicación. Por esta razón, ayuda a mitigar la mayoría de los ataques de denegación de servicio distribuido (exceptuando aquellos que utilizan un escenario de atacantes de confianza). Dicho de otro modo, los ataques de denegación de servicio distribuido basados en Internet resultan inocuos, pero un ataque de denegación de servicio iniciado desde la red de la organización continuaría siendo efectivo si el host atacante se puede autenticar y comunicar mediante IPsec.

Distinción entre el tráfico estándar y el tráfico de un ataque

Brevemente después del ataque del gusano Slammer en enero de 2003, se concluyó que las redes no habrían sido desbordadas por el tráfico del gusano si hubieran dispuesto de unas reglas sencillas que limitan el tráfico UDP al 50 por ciento del ancho de banda disponible. Los hosts infectados hubieran cubierto rápidamente ese 50 por ciento máximo del ancho de banda con el tráfico UDP, pero el resto del ancho de banda hubiera quedado disponible para el tráfico de operaciones. Los cajeros automáticos habrían continuado funcionando y los administradores podrían haber usado TCP para aplicar revisiones y propagar directivas. Aunque la directiva para limitar el tráfico UDP es simplista, estas directivas sencillas que pueden mantenerse instaladas

aportan una red de seguridad fiable.

Al utilizar IPsec para el tráfico importante, los administradores pueden aplicar una versión ligeramente más sofisticada de la directiva UDP. En condiciones normales, los administradores de red pueden supervisar la mezcla de tráfico en la red y determinar las cantidades que son tráfico UDP, tráfico TCP, tráfico ICMP (protocolo de mensajes de control de Internet), etc. Bajo presión, puede incluirse un algoritmo de cola ponderada para garantizar que el recurso se comparte según un patrón estándar. De hecho, normalmente se puede programar una directiva de estas características de forma predeterminada en los enrutadores, recopilar tendencias y estadísticas a largo plazo durante los períodos de actividad de red estándar y aplicar dichas estadísticas como colas ponderadas durante los períodos de gran congestión.

Gusanos y ataques de denegación de servicio

El pasado reciente muestra que las redes son vulnerables a los ataques de denegación de servicios, que funcionan mediante el envío de tráfico en exceso para saturar un determinado servidor o una parte concreta de una red. Una forma de ataque de denegación de servicio funciona de una forma distribuida, que dirige una serie de equipos para atacar simultáneamente a un objetivo seleccionado. La defensa en estos casos puede ser especialmente difícil.

El gusano CodeRed intentaba penetrar en primer lugar en una serie de servidores Web, los cuales se suponía que enviaban tráfico invalidante a whitehouse.gov (el dominio de la Casa Blanca en Washington DC, EE.UU.). De hecho, los mecanismos de propagación de los gusanos CodeRed, Nimda y Slammer fueron ataques de denegación de servicio contra Internet. Cada uno de los equipos infectados efectuaba cientos de miles de intentos de infección en objetivos indiscriminados, y el tráfico resultante invalidó numerosas redes locales y regionales.

IPsec protege de varias maneras frente a los ataques de denegación de servicio y proporciona un nivel adicional de protección a las víctimas potenciales del ataque. Reduce la velocidad de los atacantes obligando a realizar cálculos muy costosos y permite que los operadores de red puedan distinguir entre los distintos tipos de tráfico.

Elevación de privilegios

En este tipo de amenazas, un usuario sin privilegios logra un acceso privilegiado que le permite poner en peligro o posiblemente destruir todo el entorno

del sistema. Las amenazas de elevación de privilegios incluyen situaciones en las cuales el atacante ha superado de manera eficaz todas las defensas del sistema para explotar y dañar el sistema.

1.8.2 Otras Amenazas

No todas las amenazas encajan claramente en el modelo *STRIDE*. Los siguientes elementos muestran otras amenazas y describen su impacto potencial en una solución de aislamiento de servidor y dominio.

Seguridad física

La seguridad física implica proporcionar acceso físico a un sistema o recurso únicamente a la cantidad mínima de usuarios que lo necesitan. La seguridad física es el nivel más bajo de defensa ante la mayoría de las amenazas a la seguridad de TI. Sin embargo, en la mayoría de los ataques en el ámbito de la red, la seguridad física se omite por completo. Continúa teniendo un valor considerable como parte de un método de defensa en profundidad.

Por ejemplo, la seguridad física en forma de guardias de seguridad, cámaras en los centros de datos, controles de acceso a las ubicaciones de datos confidenciales y tarjetas de acceso o llaves para las puertas ayudan a impedir que un dispositivo de confianza resulte comprometido. El uso de varios métodos de seguridad física es importante y ayuda a impedir que se produzcan algunas de las infracciones de seguridad más graves relacionadas con los centros de datos.

Debe quedar muy claro que una seguridad física comprometida significa que todos los niveles de seguridad quedan expuestos a las amenazas. La seguridad analizada en esta solución se basa en la suposición de que la seguridad física es un asunto resuelto. Sin la seguridad física, ninguna otra medida de seguridad puede considerarse eficaz.

Seguridad de red

Una red es un sistema de quipos interconectados. La mayoría de los protocolos y servicios diseñados para las redes no se crearon teniendo en mente los potenciales propósitos malintencionados. La llegada de la informática de gran velocidad, el acceso sencillo a redes y la amplia disponibilidad de Internet han supuesto que muchos usuarios malintencionados centren sus esfuerzos en sistemas y servicios con el propósito de explotarlos o de provocar interrupciones.

Seguridad de la aplicación

La mayoría de los ataques dirigidos a aplicaciones intentan explotar las vulnerabilidades existentes en las propias aplicaciones o en el sistema operativo. Debido a que *IPsec* se implementa en la capa de red del modelo de interconexión de sistemas abiertos (*OSI*), determina si un paquete se permite o deniega mucho antes de que llegue a la aplicación.

Este comportamiento significa que IPsec no puede hacer determinaciones en el ámbito de la aplicación pero puede usarse para proporcionar seguridad al tráfico de aplicaciones en un nivel inferior.

Ingeniería social

La ingeniería social es el acto de explotar las debilidades propias del comportamiento humano para lograr el acceso a un sistema u obtener más información sobre el mismo.

Por ejemplo, un aspirante a pirata informático podría utilizar el teléfono para llamar a una determinada organización y preguntar por el nombre del supervisor que está al cargo de un proyecto en concreto. El proyecto trata del desarrollo de un producto o servicio nuevo por parte de la organización y precisamente eso es lo que interesa al atacante. Si el operador le proporciona el nombre del supervisor y quizá incluso la ubicación o la información de contacto de esa persona, el atacante dispondrá de mucha información en la que centrar sus esfuerzos.

Debido a que este tipo de ataque va dirigido al usuario del equipo, IPsec no puede proporcionar protección. De manera parecida, a un usuario malintencionado que tenga acceso a sistemas aislados y abuse de dicho acceso (atacante de confianza), se le tendrá que impedir el mal uso mediante otras tecnologías de seguridad.

1.8.3 Contramedidas o Métodos de Defensa

Tipos de Medidas de Seguridad o Contramedidas

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, eficiencia y eficacia, etc., porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variadas. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación o través de las medidas.

En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, también se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambios de las mismas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales:

- Físicas.
- Lógicas.
- Administrativas.
- Legales.

A continuación se verán las medidas de seguridad con más detalle.

Medidas Físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un *perímetro de seguridad* en nuestro sistema.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas.
- Los daños físicos por parte de agentes nocivos o contingencias.
- Las medidas de recuperación en caso de fallo.

Los tipos de controles que se pueden establecer, incluyen:

- Control de las condiciones medioambientales como ser temperatura, humedad, polvo, etc.
- Prevención de catástrofes, esto es incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.
- Vigilancia, incluye cámaras, guardias, etc.
- Sistemas de contingencia como extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.
- Sistemas de recuperación: copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.
- Control de la entrada y salida de materiales como elementos desechables, consumibles, material anticuado, etc.

Medidas Lógicas

Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad se pueden destacar los siguientes:

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la criptografía para proteger los datos y las comunicaciones.
- Uso de cortafuegos (FireWall) para proteger una red local de Internet.
- Definición de una política de copias de seguridad.
- Definición de una política de monitoreo (logging) y auditoría (auditing) del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar *medidas humanas*. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ¿A quién se le permite el acceso y uso de los recursos?.
- ¿Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?.
- ¿Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?.
- ¿Cuáles son los derechos y responsabilidades de cada usuario?.

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- El administrador del sistema y en su caso el administrador de la seguridad.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema pero sin necesidad de usarlo.
- Las personas ajenas al sistema.

Medidas Administrativas

Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.

- Establecimiento de un plan de formación del personal.

Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento es fundamental para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.

- Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.

- Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

- Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas Legales

Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.

Este tipo de medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales.

Un ejemplo de este tipo de medidas es la *LORTAD* (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal). Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medias de seguridad para su protección y las penas a imponer en caso de su incumplimiento.

1.9 Terminología, Componentes y Tipos de Criptosistemas

1.9.1 Concepto de Criptosistema

El diccionario de la Real Academia Española de la Lengua define la *criptografía* como "el arte de escribir con clave secreta o de forma enigmática". La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes.

1.9.2 Tipos de Criptosistemas

La criptografía ha venido siendo utilizada desde antiguo, fundamentalmente con fines militares. Tradicionalmente se ha hablado de dos tipos de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública.

En una infraestructura de clave pública aparecen otras autoridades, que pueden tener ciertas funciones notariales que requerirán servicios de fechado. Por ejemplo, parece natural que una Autoridad de Registro (RA), que va a ser el encargado de hacer llegar a la Autoridad Certificadora (CA) las peticiones de los usuarios remotos, sea capaz de fechar sus actos.

Los llamados sistemas criptográficos *simétricos o de clave pública* son aquellos en los que dos personas (A y B), que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A), lo cifra utilizando una determinada clave, y una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma clave que usó A para cifrarlo.

Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales inconvenientes del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.

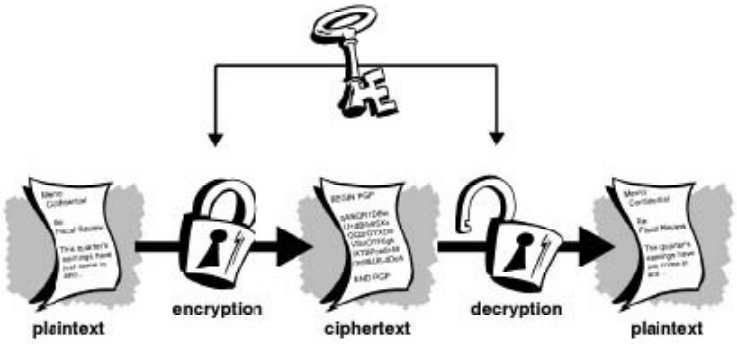

Figura 1.5: Sistema Criptográfico Simétrico

- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos no sean aptos para ser utilizados en redes abiertas como *Internet*, en las que confluyen una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Los sistemas criptográficos *asimétricos o de clave privada* se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes (privada y pública), de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es o puede ser conocida por cualquiera.
- Ambas claves, privada y pública, sirven tanto para cifrar como para descifrar mensajes.
- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es o puede ser conocida por cualquier persona, se pudiese obtener la clave privada, el

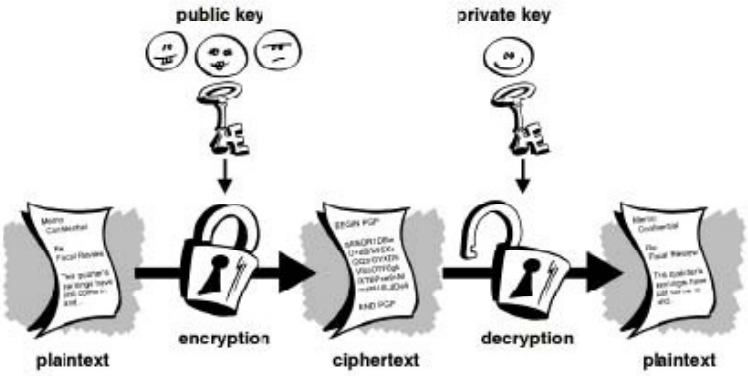

Figura 1.6: Sistema Criptográfico Asimétrico

sistema carecería de seguridad dado que cualquier podría utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

Este dato se basa en una característica de los números primos y en el llamado problema de la factorización. El problema de la factorización es la obtención a partir de un determinado producto de los factores cuya multiplicación ha dado como resultado ese producto. Los números primos (números enteros que no admiten otro divisor que no sea el 1 o ellos mismos), incluidos los números primos grandes, se caracterizan porque si se multiplica un número primo por otro número primo, da como resultado un tercer número primo a partir del cual es imposible averiguar y deducir los factores.

El criptosistema de clave pública más utilizado en la actualidad es el llamado *RSA*, creado en 1978 y que debe su nombre a sus tres creadores (Rivest, Shamir y Adleman).

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible ni inteligible.

Así se cumplen dos de los requisitos anteriormente apuntados, que son la integridad (certeza de que el mensaje no ha sido alterado) y no repudiación en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste).

El tercer requisito (identidad del emisor del mensaje) se obtiene mediante la utilización de los certificados digitales, que se analizan en otro apartado de esta guía.

1.9.3 Cifre Sus Datos Para Mantenerlos Seguros

Los usuarios suelen guardar en los equipos la información más importante y, por desgracia, los malhechores lo saben. Suponiendo que un usuario guarda en su portátil los datos de sus cuentas bancarias personales o información muy valiosa sobre empresas o clientes, y desea guardar toda esta información en un lugar seguro.

El sistema de archivos NTFS incluido en Windows XP y Vista ofrece una serie de ventajas de seguridad muy útiles que no estaban disponibles en Windows® 95, Windows 98 ni Windows Me. Una de estas ventajas es la característica de seguridad EFS (Sistema de archivos de cifrado) disponible con el sistema de archivos NTFS.

Protección contra el hurto de datos

El sistema EFS ofrece la posibilidad de cifrar archivos y carpetas. De esta forma, si alguien no autorizado consigue obtener acceso a un archivo después de sustraer, por ejemplo, un portátil o un disco, no podrá descifrar el archivo y ver su información. EFS incorpora varias capas de cifrado para incrementar la seguridad.

Cada archivo cuenta con una clave de cifrado de archivo única indispensable para poder descifrar los datos del archivo. Esta clave, que también está cifrada, sólo está en posesión de los usuarios que tienen autorización para ver los datos. EFS está integrado en el sistema de archivos, lo que dificulta aún más cualquier acceso no autorizado y, al mismo tiempo, facilita la administración por parte de los usuarios. El proceso de cifrado y descifrado de datos es totalmente transparente y prácticamente no requiere intervención por parte del usuario, que sólo debe elegir el archivo que desea cifrar.

Cuando se cifre un solo archivo, se deberá decidir si también se quiere cifrar

la carpeta que lo contiene. Si se opta por cifrar la carpeta, todos los archivos y subcarpetas que se vayan agregando a la carpeta también se cifrarán. Si se decide cifrar una carpeta, también se deberá elegir si se desea cifrar los archivos y subcarpetas ya incluidos en la carpeta.

Cifrado de carpetas

Cuando se descifre una carpeta también se deberá decidir si se descifran todos los archivos y subcarpetas incluidos en ella. Si se opta solamente por descifrar la carpeta, los archivos y subcarpetas incluidos en la carpeta permanecerán cifrados. Sin embargo, los archivos y subcarpetas nuevos no se cifrarán automáticamente.

Para cifrar un archivo o una carpeta

1. Se debe abrir el Explorador de Windows (hacer clic en Inicio, Todos los programas, Accesorios y Explorador de Windows).
2. Hacer clic con el botón secundario en el archivo o la carpeta que se desee cifrar y, a continuación, hacer clic en Propiedades.
3. En la ficha General, hacer clic en Avanzado.
4. Activar la casilla de verificación Cifrar contenido para proteger datos.

Los archivos o carpetas comprimidos no se pueden cifrar. Si se intenta cifrar un archivo o carpeta comprimido, se descomprimirá.

Los archivos marcados con el atributo Sistema no pueden cifrarse, al igual que los archivos que se encuentran en la estructura de directorios raíz del sistema.

Para descifrar un archivo o una carpeta

Los pasos son los siguientes:

1. Se debe abrir el Explorador de Windows.
2. Hacer clic con el botón secundario en el archivo o carpeta cifrado y, a continuación, hacer clic en Propiedades.
3. En la ficha General, hacer clic en Avanzado.

4. Desactivar la casilla de de verificación Cifrar contenido para proteger datos.

Capítulo 2

Controles de Acceso

2.1 ¿Qué Cosas Hace Un Sistema Seguro?

Un tratamiento total de seguridad incluye aspectos de la seguridad del computador distintos a los de la seguridad de los Sistemas Operativos.

Debe incluir seguridad externa e interna [5, Tan96]:

- La *seguridad externa* debe asegurar la instalación computacional contra intrusos y desastres como incendios e inundaciones. Concedido el acceso físico, el Sistema Operativo debe identificar al usuario antes de permitirle el acceso a los recursos: seguridad de la interfaz del usuario.
- La *seguridad interna* trata de los controles incorporados al hardware y al Sistema Operativo para asegurar la confiabilidad, operabilidad y la integridad de los programas y datos.

La seguridad externa consiste en:

- Seguridad física, incluye protección contra desastres y protección contra intrusos. Son importantes los mecanismos de detección: detectores de humo, sensores de calor, detectores de movimiento, etc.
- Trata especialmente de impedir la entrada a intrusos, utilizando sistemas de identificación física como: tarjetas de identificación, sistemas de huellas digitales, identificación por medio de voz, etc.

2.2 Control de Acceso al Sistema

2.2.1 Administrador de Seguridad

Se llama Administrador de Seguridad todo aquel que posee un nivel de acceso superior al del propio Usuario para realizar tareas de instalación/desinstalación, mantenimiento y soporte del sistema.

En función del volumen de Pc's, y la dispersión geográfica de los mismos, puede ser necesario designar varias clases de administradores. Cada clase tendrá un nivel muy concreto de responsabilidad frente al sistema ya que todos los sistemas, poseen la capacidad de distinguir automáticamente, en función de la identificación, el grado de profundidad a que pueden tener acceso o las puertas que están capacitados para abrir. También pueden designarse privilegios temporales de administrador para realizar tareas muy concretas de mantenimiento en un momento dado [4, Tan87].

2.3 Control de Acceso a Datos

Lo fundamental de la seguridad interna es controlar el acceso a los datos almacenados. **Deitel

Los derechos de acceso definen qué acceso tienen varios sujetos a varios objetos. Los sujetos acceden a los objetos.

Los objetos son entidades que contienen información, pueden ser:

- Concretos, como discos, cintas, procesadores, almacenamiento, etc.
- Abstractos, como estructuras de datos, de procesos, etc.

Los objetos están protegidos contra los sujetos. Las autorizaciones a los sujetos se conceden a los sujetos. Los sujetos pueden ser varios tipos de entidades, como usuarios, procesos, programas, otras entidades, etc.

Los derechos de acceso más comunes son:

- Acceso de lectura.

- Acceso de escritura.
- Acceso de ejecución.

Una forma de implementación es mediante una matriz de control de acceso con:

- Filas para los sujetos.
- Columnas para los objetos.
- Celdas de la matriz para los derechos de acceso que un usuario tiene a un objeto.

2.3.1 El Control de Acceso Como Medio Para Restringir el Uso de los Archivos

El sistema de archivos NTFS disponible en las últimas versiones de Windows proporciona varias ventajas de seguridad con respecto a las versiones anteriores que no contaban con NTFS. Una de estas ventajas es el control de acceso. Esta medida de seguridad permite limitar el acceso de los usuarios a los datos de un equipo o red mediante el uso de listas de control de acceso de Windows XP o Vista en unidades con formato NTFS. Las características de control de acceso permiten restringir el acceso a un usuario, equipo o grupo de usuarios determinado.

Definición de permisos en archivos y carpetas

Los permisos se definen para determinar el tipo de acceso que se concede a un usuario o grupo de usuarios. Por ejemplo, para el archivo contabilidad.dat se puede otorgar permisos de lectura y escritura a todo el grupo financiero. Al establecer permisos también se especifica el nivel de acceso que se concede a los grupos y usuarios. Es decir, se puede permitir que un usuario determinado pueda leer el contenido de un archivo, permitir que otro usuario pueda realizar cambios en ese mismo archivo e impedir que el resto de usuarios puedan obtener acceso al archivo.

Para las impresoras también es posible definir permisos similares. De esta forma, se puede conceder los permisos necesarios para que algunos usuarios puedan configurar la impresora y para que otros individuos únicamente puedan

utilizarla para imprimir. Para cambiar los permisos de un archivo o carpeta, es necesario ser el propietario del archivo o carpeta, o bien disponer de los permisos necesarios para poder realizar estos cambios.

Permisos de grupos

Para obtener un resultado óptimo, es aconsejable asignar permisos a grupos en lugar de a usuarios. De esta forma, no es necesario mantener individualmente el control de acceso de cada usuario. Si las circunstancias lo permiten, debe asignar Control total en lugar de permisos individuales, o utilizar Denegar para excluir un subconjunto de un grupo con permisos Permitidos o para excluir un permiso especial si ya se ha concedido control total a un usuario o grupo.

El tipo de permisos que se puede conceder depende del tipo de objeto. Por ejemplo, los permisos de un archivo son distintos de los permisos de una clave de registro, aunque algunos de ellos, como los que se mencionan a continuación, son comunes:

- Permisos de lectura.
- Permisos de modificación.
- Cambiar propietario.
- Eliminar.

Para establecer, ver, cambiar o eliminar los permisos de un archivo o carpeta se deben seguir las instrucciones que se listan a continuación:

1. Abrir el Explorador de Windows (hacer clic en Inicio, Todos los programas, Accesorios y Explorador de Windows).
2. Buscar el archivo o carpeta para el que desea establecer los permisos.
3. Hacer clic con el botón secundario en el archivo o la carpeta, a continuación hacer clic en Propiedades y, por último, en la ficha Seguridad.
4. Realizar una de estas acciones:
   (a) Para establecer permisos para un grupo o un usuario que no consta en el cuadro Nombres de grupos o usuarios, hacer clic en Agregar.

Escribir el nombre del grupo o usuario para el que desee establecer los permisos y, a continuación, hacer clic en Aceptar. (Al agregar un nuevo usuario o grupo, el usuario o grupo en cuestión tendrá, de forma predeterminada, permisos de Lectura y Ejecución, Mostrar el contenido de la carpeta y Lectura.)

(b) Para cambiar o eliminar los permisos de un grupo o usuario existente, hacer clic en el nombre del grupo o usuario.

5. Realizar una de estas acciones:

   (a) Para conceder o denegar un permiso, en el cuadro Permisos para usuario o grupo, seleccionar la casilla de verificación Permitir o Denegar.

   (b) Para eliminar el grupo o usuario del cuadro Nombres de grupos o usuarios, hacer clic en Quitar.

6. Si las casillas de verificación situadas debajo de Permisos para usuario o grupo están sombreadas, o si el botón Quitar no está disponible, significa que el archivo o la carpeta ha heredado los permisos de la carpeta principal.

Para ver la ficha Seguridad:

- Abrir Opciones de carpeta en el Panel de control (hacer clic en Inicio y, a continuación, en Panel de control, hacer doble clic en Opciones de carpeta).
- En la ficha Ver, bajo Configuración avanzada, desactivar la casilla Utilizar uso compartido simple de archivos [recomendado].

2.3.2 Métodos de Cifra Poligrámica

Estos métodos de criptografía efectúan el cifrado por grupo de caracteres en lugar del caracter individual. Según su agrupación se clasifican en:

- *Diagrámicos:* El cifrado se realiza en grupos de dos caracteres.
- *Trigrámica:* El ciframiento es en grupo de tres caracteres.

2.4 Otras Transformaciones Criptográficas: La Firma Digital

2.4.1 ¿Qué Es la Firma Digital?

La firma digital puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

La aparición y desarrollo de las redes telemáticas, como Internet, ha supuesto la posibilidad de intercambiar entre personas distantes geográficamente mensajes de todo tipo, incluidos los mensajes de contenido contractual. Estos mensajes plantean el problema de acreditar tanto la autenticidad como la autoría de los mismos.

Concretamente, para que dos personas, puedan intercambiar entre ellas mensajes electrónicos de carácter comercial que sean mínimamente fiables y puedan, en consecuencia, dar a las partes contratantes la confianza y la seguridad que necesita el tráfico comercial, esos mensajes deben cumplir los siguientes requisitos:

1. *Identidad*, que implica poder atribuir de forma indubitada el mensaje electrónico recibido a una determinada persona como autora del mensaje.
2. *Integridad*, que implica la certeza de que el mensaje recibido por B (receptor) es exactamente el mismo mensaje emitido por A (emisor), sin que haya sufrido alteración alguna durante el proceso de transmisión de A hacia B.
3. *No repudio o no rechazo* en origen, que implica que el emisor del mensaje (A) no pueda negar en ningún caso que el mensaje ha sido enviado por él.

Pues bien, la firma digital es un procedimiento técnico que basándose en técnicas criptográficas trata de dar respuesta a esa triple necesidad apuntada anteriormente, a fin de posibilitar el tráfico comercial electrónico.

Por otra parte, a los tres requisitos anteriores, se une un cuarto elemento, que es la *confidencialidad*, que no es un requisito esencial de la firma digital sino accesorio de la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

2.4.2 ¿En Qué se Basa la Firma Digital?

La firma digital se basa en la utilización combinada de dos técnicas distintas, la criptografía asimétrica o de clave pública para cifrar mensajes y el uso de las llamadas funciones hash o funciones resumen.

Las Funciones Hash

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas funciones hash o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje resumen o hash, que también tendrá una dimensión fija y constante de 160 bits.Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

2.4.3 Los Sellos Temporales

Finalmente, en el proceso de intercambio de mensajes electrónicos es importante que, además de los elementos o requisitos anteriormente analizados, pueda saberse y establecerse con certeza la fecha exacta en la que los mensajes han sido enviados. Esta característica se consigue mediante los llamados sellos temporales o “time stamping”, que es aquella función atribuida generalmente a los Prestadores de Servicios de Certificación mediante la cual se fija la fecha

de los mensajes electrónicos firmados digitalmente.

2.4.4 La Confidencialidad de los Mensajes

En ocasiones, además de garantizar la procedencia de los mensajes electrónicos que se intercambian por medio de Internet y la autenticidad o integridad de los mismos, puede ser conveniente garantizar también su confidencialidad. Ello implica tener la certeza de que el mensaje enviado por A (*emisor*) únicamente será leído por B (*receptor*) y no por terceras personas ajenas a la relación que mantienen A y B.

En tales casos, también se acude al cifrado del mensaje con el par de claves, pero de manera diferente al mecanismo propio y característico de la *firma digital*.

Para garantizar la confidencialidad del mensaje, el *cuerpo* del mismo (no el hash o resumen) se cifra utilizando la clave pública de B (receptor), quien al recibir el mensaje lo descifrará utilizando para ello su clave privada (la clave privada de B). De esta manera se garantiza que únicamente B pueda descifrar el cuerpo del mensaje y conocer su contenido.

2.4.5 La Obtención del Par de Claves y de los Certificados Digitales

¿Dónde puede obtener una persona el par de claves?

La *firma digital* se genera mediante la utilización de un par de claves de cifrado (pública y privada), que se utilizan para cifrar y descifrar los mensajes. A diferencia de la firma autógrafa, que es de libre creación por cada individuo y no necesita ser autorizada por nadie ni registrada en ninguna parte para ser utilizada, la firma digital, y más concretamente el par de claves que se utilizan para firmar digitalmente los mensajes, no pueden ser creados libremente por cada individuo.

En principio, cualquier persona puede dirigirse a una empresa informática que cuente con los dispositivos necesarios para generar el par de claves y solicitar la creación de dicho par de claves. Posteriormente, con el par de claves creado para una persona determinada, ésta se dirigiría a un *Prestador de Servicios de Certificación* para obtener el *certificado digital* correspondiente

a ese par de claves.

Sin embargo, en la práctica los Prestadores de Servicios de Certificación cumplen ambas funciones: crean el par de claves para una persona y expiden el certificado digital correspondiente a ese par de claves.

2.4.6 ¿Qué Son los Certificados Digitales?

La utilización del par de claves (privada y pública) para cifrar y descifrar los mensajes permite tener la certeza de que el mensaje que B recibe de A y que descifra con la clave pública de A, no ha sido alterado y proviene necesariamente de A. Pero ¿Quién es A?.

Para responder de la identidad de A (emisor) es necesario la intervención de un tercero, que son los llamados *Prestadores de Servicios de Certificación*, cuya misión es la de emitir los llamados certificados digitales o certificados de clave pública.

Un certificado digital es un archivo electrónico que tiene un tamaño máximo de 2 Kilobytes y que contiene los datos de identificación personal de A (emisor de los mensajes), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta.

Los certificados digitales tienen una *duración determinada*, transcurrido un tiempo deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si se sabe que el mensaje ha sido cifrado con la clave privada de esa persona, también se sabe quién es la persona titular de esa clave privada.

2.4.7 ¿Cómo se Obtiene el Dispositivo para Firmar Digitalmente un Mensaje?

El *proceso de obtención* de los elementos necesarios para *firmar digitalmente mensajes* (par de claves y certificado digital) es el siguiente:

1. Dirigirse a una empresa o entidad que tenga el carácter de Prestador de Servicios de Certificación y solicitar de ellos el par de claves y el certificado digital correspondiente a las mismas. Generalmente, se puede acudir a dicha entidad bien personalmente o por medio de internet utilizando la página web del Prestador de Servicios de Certificación.

2. El prestador de Servicios de Certificación comprobará la identidad, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), para lo cual se deberá exhibir el D.N.I. y en el caso de ser el representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, se debe acreditar documentalmente el cargo y sus facultades.

3. El prestador de Servicios de Certificación crea con los dispositivos técnicos adecuados el par de claves pública y privada y genera el certificado digital correspondiente a esas claves.

4. El prestador de Servicios de Certificación entrega una tarjeta semejante a una tarjeta de crédito que tiene una banda magnética, aunque actualmente se vienen sustituyendo por las tarjetas denominadas "smartcard" que incorporan un chip, en la que están grabados tanto el par de claves como el certificado digital. El acceso al par de claves y al certificado digital grabados en la tarjeta está protegido mediante una clave como las que se utilizan en las tarjetas de crédito o en las tarjetas de cajero automático. En otras ocasiones, en lugar de la tarjeta el Prestador de Servicios de Certificación deja almacenado el certificado digital en su propia página web, a fin de que el destinatario copie el archivo y lo instale en su ordenador.

5. Con esa tarjeta y un lector de tarjetas smartcard (o de banda magnética si fuera el caso) adecuado conectado al ordenador personal, se podrá leer y utilizar la información grabada en la tarjeta para firmar digitalmente los mensajes electrónicos que se envíen a otras personas.

2.4.8 ¿Cómo Funciona la Firma Digital?

El proceso de firma digital de un mensaje electrónico comprende en realidad dos procesos sucesivos: la firma del mensaje por el emisor del mismo y la verificación de la firma por el receptor del mensaje. Estos dos procesos tienen lugar de la manera que se expresa a continuación.

Firma digital de un mensaje electrónico

1. El emisor crea o redacta un mensaje electrónico determinado (por ejemplo, una propuesta comercial).
2. El emisor aplica a ese mensaje electrónico una función hash (algoritmo), mediante la cual obtiene un resumen de ese mensaje.
3. El emisor cifra ese mensaje resumen utilizando su clave privada.
4. El emisor envía al receptor un correo electrónico que contiene los siguientes elementos:
   (a) El *cuerpo del mensaje*, que es el mensaje en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública del receptor.
   (b) La *firma del mensaje*, que a su vez se compone de dos elementos:
      i. El *hash o mensaje resumen* cifrado con la clave privada del emisor.
      ii. El *certificado digital del emisor*, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

Verificación por el receptor de la firma digital del mensaje

1. El receptor recibe el correo electrónico que contiene todos los elementos mencionados anteriormente.
2. El receptor en primer lugar descifra el certificado digital del emisor, incluido en el correo electrónico, utilizando para ello la clave pública del Prestador de Servicios de Certificación que ha expedido dicho certificado. Esa clave pública la tomará el receptor, por ejemplo, de la página web del Prestador de Servicios de Certificación en la que existirá depositada dicha clave pública a disposición de todos los interesados.
3. Una vez descifrado el certificado, el receptor podrá acceder a la clave pública del emisor, que es uno de los elementos contenidos en dicho certificado. Además podrá saber a quién corresponde dicha clave pública, dado que los datos personales del titular de la clave (emisor) constan también en el certificado.

4. El receptor utilizará la clave pública del emisor obtenida del certificado digital para descifrar el hash o mensaje resumen creado por el emisor.

5. El receptor aplicará al cuerpo del mensaje, que aparece en claro o no cifrado, que también figura en el correo electrónico recibido, la misma función hash que utilizó el emisor con anterioridad, obteniendo igualmente el receptor un mensaje resumen. Si el cuerpo del mensaje también ha sido cifrado para garantizar la confidencialidad del mismo, previamente el receptor deberá descifrarlo utilizando para ello su propia clave privada.

6. El receptor comparará el mensaje resumen o hash recibido del emisor con el mensaje resumen o hash obtenido por ella misma. Si ambos mensajes resumen o hash coinciden totalmente significa lo siguiente:

   (a) El mensaje no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.

   (b) El mensaje resumen descifrado por el receptor con la clave pú blica del emisor ha sido necesariamente cifrado con la clave privada del emisor y, por tanto, proviene necesariamente del emisor.

   (c) Como el certificado digital nos dice quién es el emisor, se puede concluir que el mensaje ha sido firmado digitalmente por el emisor, siendo éste una persona con identidad determinada y conocida.

   (d) Por el contrario, si los mensajes resumen no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión, y si el mensaje resumen descifrado por el receptor es ininteligible quiere decir que no ha sido cifrado con la clave privada del emisor. En resumen, que el mensaje no es auténtico o que el mensaje no ha sido firmado por el emisor sino por otra persona.

   (e) Finalmente, hay que tener en cuenta que las distintas fases del proceso de firma y verificación de una firma digital que han sido descritas no se producen de manera manual sino automática e instantánea, por el simple hecho de introducir la correspondiente tarjeta magnética en el lector de tarjetas de nuestro ordenador y activar el procedimiento.

Capítulo 3

Planeamiento y Administración de Sistemas Seguros

3.1 Decisiones Generales de Planeamiento y Administración

El Planeamiento Estratégico de Sistemas es una actividad esencial para el desarrollo de sistemas seguros. Sus beneficios se listan a continuación.

- Alinear los objetivos de la organización con estrategias de Tecnología de la Información.
- Integrar las diferentes áreas de la organización bajo una única arquitectura de información.
- Definir los proyectos que implanten las estrategias tecnológicas.
- Administrar los riesgos de cada estrategia y los presupuestos de una manera metódica.
- Definir mejores estructuras organizacionales de sistemas.
- Definir indicadores para evaluar la efectividad de cada estrategia.

- Administrar de una manera ordenada y consensuada las nuevas estrategias con los problemas del día a día.
- Facilitar proyectos de mejoras a los procesos de desarrollo y mantenimiento de sistemas.

Se debe Integrar efectivamente la estrategia con el Plan de TI mediante la participación activa y simultánea de directivos de TI y de directivos de cada una de las áreas.

3.2 Planeamiento y Control de Proyectos

Es el proceso que permite manejar efectivamente los recursos, tiempos y presupuestos del proyecto. Para lograr esto se necesita acceso a la información y a las formas de modelar la misma para maximizar la efectividad y minimizar los riesgos [1, KIN98].

Básicamente, el proceso consta de las siguientes actividades:

- *Manejo del cronograma (planificación y control)*: Construcción y revisión del plan, identificación de tareas completadas y de las no completadas de acuerdo a lo previsto, verificación de la asignación de recursos, replanificación, evaluación del camino crítico, ajustes al plan.
- *Manejo de riesgos:* Planificación y control de los riesgos.
- *Manejo del cambios:* Procedimiento de solicitud de cambios, autorización y seguimiento de los cambios.
- *Manejo de las comunicaciones:* Agendas de reunión, reportes del proyecto, otras comunicaciones especiales,
- *Manejo de la calidad:* Entregables, requerimientos de calidad, actividades de control de la calidad, actividades de aseguramiento de la calidad, seguimiento de errores.
- *Manejo de problemas:* Proceso para manejo y seguimiento de incidentes, procedimiento de escalamiento.
- *Biblioteca del proyecto:* Definición, procedimientos y estándares (control de versiones, distribución, archivo o destrucción), estructura de la biblioteca.

3.3 División de Roles o Tareas

El Administrador de Seguridad posee un nivel de acceso superior al del usuario para realizar tareas de instalación/desinstalación, mantenimiento y soporte del sistema.

Un sistema de seguridad puede definirse como una serie de elementos físicos y lógicos que ajustan, para cada usuario, su capacidad de generar y manipular información a la responsabilidad real que ha sido asignada a cada puesto de trabajo.

Así, dentro de un sistema de seguridad, cada usuario ha de tener su parcela de trabajo perfectamente definida y delimitada, y por encima de ellos, para solucionar incidencias, instalar nuevas aplicaciones y asegurar que la comunicabilidad con el exterior siempre obedezca a los intereses y objetivos por los cuales se instala el sistema, debe existir la figura del administrador capacitada para abrir las puertas necesarias cuando así se precise y responsable de todo lo que en la Pc ocurra durante el tiempo en que las puertas permanezcan abiertas.

La implementación de un sistema de seguridad, significa, también, minimizar los puntos de riesgo. No debe caerse en la simpleza de pretender eliminarlos absolutamente todos. Esto último equivaldría a cerrar a "cal y a canto" cualquier intersticio posible dejando acumulada toda la responsabilidad a un solo Administrador. La instalación de un sistema de seguridad pretende limitar los puntos de riesgo, y los que conscientemente se decidan dejar que sean controlables por otros medios.

Por ejemplo, un parque de 5.000 Pc's tendrá 5.000 puntos de riesgo, nombrando a un Director de Seguridad y 50 Soportes, habremos disminuido a 51 el número de puntos de riesgo, que además pueden ser controlados por otras vías.

3.3.1 Clases de Administradores

Pueden haber varias clases y categorías de administradores permanentes:

- Director de seguridad.
- Soporte de seguridad.

- Instalador de seguridad.
- Auditor de seguridad.

Además de estos, pueden designarse administradores temporales por tiempo y por funciones si el sistema lo permite.

A continuación se definen las dos clases de administrador de seguridad, que deben existir cuando hay un gran parque de usuarios que atender.

El Soporte de Seguridad

Esta es una figura cercana al usuario que será el verdadero brazo ejecutor de la instalación y buen funcionamiento del sistema de seguridad en los equipos bajo su custodia, sin embargo no podrá, bajo su responsabilidad, abrir ninguna puerta a petición directa del usuario.

Todo cuanto haya de hacer en la Pc relativo a la seguridad debe venir avalado por una autorización del Administrador de Seguridad o de la jerarquía que corresponda en el organigrama del sistema. Autorización que siempre debe ser por escrito.

Funciones

- Instalar el sistema de seguridad en los Pc's bajo su custodia.
- Desinstalar el sistema de seguridad de algún puesto de trabajo, cuando el Director de Seguridad, por necesidades justificadas, así lo autorice. El Soporte de Seguridad deberá controlar la Pc durante todo el tiempo que no tenga instalado el sistema. Además:
- Proporcionar soporte técnico al usuario final.
- Restablecer la Password de usuario si este la pierde, o se ausenta y su máquina debe ser utilizada por otro usuario previa autorización de quién corresponda.
- Informar al Director de Seguridad de cualquier anomalía al sistema.
- Ejecutar en su Pc las conversiones de formato autorizadas.

Conocimientos

- Perfecto conocimiento técnico de ofimática.
- Conocimiento de las funcionalidades del sistema de seguridad.
- Instalar y desinstalar los productos (no debe conocer las claves de cifrado si las hay).
- El soporte no debe revelar a nadie su password de soporte (hasta puede ser conveniente que cada soporte posea una password distinta para su grupo de Pc's) y debe controlar el Pc en caso de que se desinstale, temporalmente, la seguridad.

El Director de Seguridad

Será el máximo responsable del cumplimiento de los objetivos de seguridad fijados, dirigirá el diseño del sistema, tanto a nivel de programas a instalar como la organización a implantar. De él dependerán funcional u orgánicamente los soportes de seguridad y otros administradores.

Por razones operativas quizás pueda ser conveniente delegar la responsabilidad de autorizar determinadas operaciones a los jefes de dependencia. En el caso de que así se decidiera, los soportes de seguridad, aunque seguirán dependiendo y reportando al director de seguridad, aquellos recibirán de los jefes de dependencia, las autorizaciones solicitadas por los usuarios.

Funciones

- Diseñar y configurar todo el sistema.
- Determinar los identificadores de los administradores.
- Determinar las claves de cifrado de discos duros y disquetes.
- Guardar claves y palabras en un sobre y en un lugar seguro.
- Distribuir los archivos de configuración a los soportes de seguridad.
- Auditar, por muestreo aleatorio en el tiempo, que las claves no son violadas y en general que todo el sistema funciona según lo previsto.

- En caso de violación en algún punto, debe tomar las medidas oportunas para restablecer la seguridad en todo el conjunto.
- Proporcionar soporte técnico y organizativo a los soportes de seguridad.

Conocimientos Técnicos

- Prefecto conocimiento técnico de la ofimática.
- Perfecto conocimiento técnico de los productos de seguridad instalados.

Jerarquía

Genéricamente se denomina jerarquía a los encargados, no informáticos, cuya misión es la de conceder determinadas autorizaciones a los usuarios. Por ejemplo un Director de Departamento o un Jefe de Sección.

Sus funciones no son informáticas y su formación respecto al sistema de seguridad instalado, es puramente funcional.

Bibliografía

[1] J. H. Kingston. *Algorithms and Data Structures. Desing, Correctnes, Analysis. Second Edition.* Addison-Wesley, 1998.

[2] David L. la Red Martínez. *Sistemas Operativos.* EUDENE, Argentina, 2004.

[3] N.Ñegroponte. *El Mundo Digital.* Ediciones B, Barcelona-España, 1995.

[4] A. S. Tanenbaum. *Operating Systems: Design And Implementation.* Prentice Hall, NJ-USA, 1987.

[5] A. S. Tanenbaum. *Sistemas Operativos Distribuidos.* Prentice Hall Hispanoamericana, S.A., México, 1996.

Índice de Materias