

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

MONOGRAFIA

SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA



Noelia Desiree Litwak - L.U.: 30550
Jaquelina Edit Escalante- L.U.: 32885

Director: Mgter. David Luis la Red Martínez

Licenciatura en Sistemas de Información
Corrientes - Argentina

2004

Índice General

1	Introducción	1
2	Seguridad Informática	15
2.1	Definición	15
2.1.1	Análisis del objetivo de la seguridad informática [1] . . .	17
2.1.2	Principios básicos para la seguridad	18
2.1.3	La seguridad como problema cultural	19
2.1.4	La seguridad como proceso	20
2.1.5	Factores que afectan a los sistemas de información . . .	20
2.2	Seguridad Física	21
2.3	Seguridad Lógica	23
2.4	Vulnerar para proteger	24
2.5	Controles de acceso	25
2.5.1	Acceso - Uso - Autorización	26
2.5.2	Identificación de las amenazas	26
2.5.3	Delito Informático	28
2.5.4	Riesgos “No naturales”	28
2.5.5	Estrategias de seguridad	29
2.5.6	Otras medidas de seguridad	32
2.5.7	Penetration Test, Ethical Hacking o pueba de vulnerabilidad	37
2.5.8	HoneyPots, HoneyNets	38
2.5.9	Firewalls	39
2.5.10	Routers y Bridges	40
3	Criptografía	42
3.0.11	Conceptos Previos	43
3.0.12	Sistemas Criptográficos	44

3.0.13	Gestión de Claves	46
3.0.14	Distribución Simétrica de Claves Simétricas	46
3.0.15	El Acuerdo de distribución	47
3.0.16	Distribución Asimétrica de Claves Simétricas	47
3.1	Criptografía Simétrica	48
3.1.1	Cifrado de Flujo	51
3.1.2	Cifrado en Bloque	52
3.1.3	Cifrado de Feistel	52
3.1.4	El Cifrador de César	52
3.1.5	DES (Data Encryption Standar) [2]	54
3.1.6	Seguridad en DES	55
3.1.7	Variantes del DES	57
3.1.8	DES Múltiple	57
3.1.9	IDEA (International Data Encryption Algorirhm)	57
3.2	Criptografía Asimétrica	58
3.2.1	RSA	59
3.2.2	Seguridad RSA	61
3.2.3	Algoritmo Asimétrico ElGamal	62
3.2.4	Digital Signature Algorithm (DSA)	63
3.2.5	Planteamiento de Casos	63
3.2.6	Funciones Hash	65
3.2.7	Firmas Digitales	67
3.2.8	Ventajas de la Firma Digital	69
3.2.9	Funcionamiento de las Firmas Digitales	71
3.2.10	Seguridad de la Firma Digital	73
3.2.11	Aplicación de la Firma Digital	73
3.2.12	Entidades de Certificación	74
3.2.13	Software Easy Sign	77
3.2.14	Principales funciones de la Firma	77
3.2.15	Infraestructura de la Firma Digital	77
3.2.16	Organismo Licenciante	78
3.2.17	Organismo Auditante	78
3.2.18	Autoridades Certificantes Licenciadas	79
3.2.19	Procedimientos	79
3.2.20	Laboratorio de Firma Digital	79
3.2.21	Comprobación de la entidad del firmante	80
3.2.22	Certificado Digital Propio	80
3.2.23	Obtención de una Firma Digital	81
3.2.24	Autoridad Certificante Licenciada	81

<i>ÍNDICE GENERAL</i>	iv
3.2.25 Certificados Digitales	84
Bibliografía	86
Índice de Materias	87

Índice de Figuras

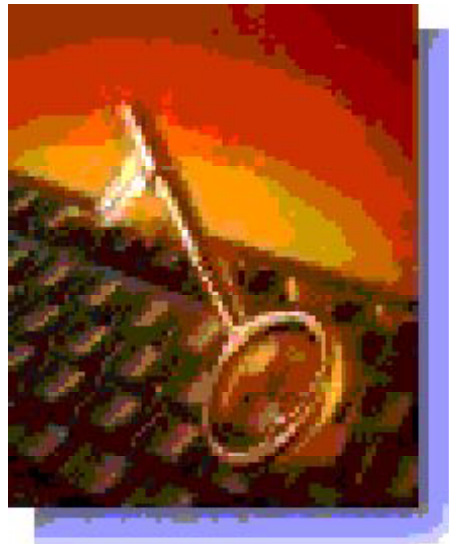
2.1	Amenazas Frecuentes.	22
2.2	Tipos de atacantes.	27
2.3	Esquema de Firewall.	40
3.1	Sistema Criptográfico.	43
3.2	Comunicación Insegura.	45
3.3	Proceso Criptográfico.	48
3.4	Igual Clave o LLave.	49
3.5	Envío inseguro de la Clave.	50
3.6	Cifrado de Flujo.	51
3.7	Cifrado de Feistel.	53
3.8	Algoritmo DES.	56
3.9	Primer Caso.	63
3.10	Segundo Caso.	64
3.11	Tercer Caso.	66
3.12	Autoridad Licenciante Certificada.	81
3.13	Autoridad Licenciante.	82
3.14	Autoridad Licenciante.	82
3.15	Energía Atómica.	83

Capítulo 1

Introducción

El amplio desarrollo de las nuevas tecnologías informáticas están ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

Esto nos llama a reflexionar sobre la seguridad que existe en nuestros sistemas informáticos. Muchas personas confunden el término seguridad, y no le dan la importancia que realmente merece.



Vamos a comenzar haciendo una distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección.

Si bien los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad, no son suficientes. Las políticas definen qué hay que hacer (qué datos y recursos deben protegerse y de quién), y los mecanismos determinan cómo hay que hacerlo. Esta separación es importante en términos de flexibilidad, puesto que las políticas pueden variar en el tiempo y de una organización a otra. Los mismos mecanismos, si son flexibles, pueden usarse para implementar distintas políticas.

Los mecanismos que ofrece el sistema operativo necesariamente deben complementarse con otros de carácter externo. Por ejemplo, impedir el acceso físico de personas no autorizadas a los sistemas es un mecanismo de protección cuya implementación no tiene nada que ver con el sistema operativo.

Así un aspecto importante de la seguridad es el de impedir la pérdida de información, la cual puede producirse por diversas causas: fenómenos naturales, guerras, errores de hardware o de software, o errores humanos. La solución es una sola: mantener la información respaldada, de preferencia en un lugar lejano; y otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos, como ser lectura de datos, modificación de datos, destrucción de datos o uso de recursos.

Aquí el sistema operativo juega un rol fundamental, ofreciendo mecanismos de autorización y autenticación.

Protección absoluta contra uso malicioso de los sistemas es imposible, pero si los costos de violar un sistema son superiores a los potenciales beneficios que se pueden obtener, entonces el sistema puede considerarse seguro. El problema es que esa protección no obstaculice el uso del sistema por parte de usuarios autorizados. Demasiada seguridad podría ser contraproducente si es muy engorrosa para los usuarios, pues estos tenderán a eludir los procedimientos para facilitarse la vida.

La difusión masiva de mecanismos que procuran brindar seguridad a la transmisión de información entre computadoras surge fundamentalmente a partir del desarrollo del comercio electrónico en redes abiertas como Internet.

El éxito del comercio electrónico se basa en la aparición de un mercado

global (la red), en el que el contacto físico ha sido relegado y reducido a su mínima expresión.

El comercio electrónico o digital consiste en la transformación de las transacciones y procesos basados en papel en un proceso digital en que la palabra impresa en papel es reemplazada por el lenguaje de las computadoras (unos y ceros, números binarios). Para que dicho mercado global se convierta en un medio apropiado para el comercio debe existir una forma de asegurar que los emisores y receptores de dichos ceros y unos puedan ser identificados con cierto grado de certeza y que la información transmitida no sufra alteraciones.

Para comprender el tipo de solución que se necesita a efectos de implementar una infraestructura global de información es indispensable entender el tipo de tráfico comercial que desea transportarse por las redes. El comercio minorista es una pequeña parte del futuro del comercio digital. Existe un espectro de servicios (legales, financieros, de salud) que pueden ser ofrecidos más eficientemente con la ayuda de las redes abiertas.

Internet constituye el ejemplo predominante y más importante en el mundo de una red abierta, existiendo gran cantidad de negocios que se realizan sin mayores complicaciones por su intermedio. Incluso se ha dicho que este tipo de comercio florecerá en redes abiertas sin necesidad de grandes inversiones en tecnología para proveer un alto grado de certeza en la integridad de los mensajes transmitidos, seguridad y autenticación. Pero estos argumentos sólo son válidos para este pequeño sector del comercio, y no para otros sectores, como el de salud, el sector financiero y el legal, en los que la información que se almacena o se transmite tiene una importancia tal que requieren un mayor grado de cuidado.



A efectos de que los sistemas abiertos puedan ser utilizados para transportar este tipo de información, es indispensable poder identificar las personas que participan en las comunicaciones, independientemente del lugar físico utilizado.

La tecnología requerida para lograr la seguridad a que se ha hecho referencia ya existe en la forma de la firma digital, basada en la criptografía de clave pública.

Otro de los aspectos decisivos para afianzar el comercio electrónico en Internet está constituido por el entorno jurídico, es decir, las leyes y decretos que sirven de soporte para las transacciones, e introducen el concepto de seguridad jurídica en el mercado digital.

Hay una opinión generalizada de que, si ya es complicado, en la vida real, demostrar la existencia de una deuda que no se ha formalizado en un título ejecutivo, la dificultad probatoria será mayor en una plataforma contractual en la que el consentimiento se transmite en forma de bits.

Es evidente que la eficacia del marco jurídico radica en su uniformidad, ya que si su contenido difiere en cada provincia, será difícil su aplicación a un entorno global como Internet. Por ello, el esfuerzo a realizar a partir de ahora deberá centrarse en la consecución de un modelo supraprovincial, que pueda ser implantado de manera uniforme en legislación nacional.

En definitiva para subsanar problemas relativos a la seguridad, surgieron

distintos métodos o estrategias, siendo uno de los más antiguos pero actualmente utilizados la criptografía.

La criptografía ha sido usada a través de los años para mandar mensajes confidenciales, proviene del griego *kryptos* (esconder) y *gráphein* (escribir), es decir “*Escritura escondida*” y su principal objetivo es que sólo dos personas autorizadas puedan intercambiar información sin que una tercera persona no autorizada sea capaz de descifrar la información.

El mecanismo más básico es el denominado criptosistema o algoritmo de encriptación, que define dos transformaciones:

- La encriptación: conversión el texto en claro (plaintext) en el texto cifrado o criptograma (ciphertext) mediante el empleo de la denominada clave de encriptación.
- La desencriptación: proceso inverso que emplea la llamada clave de desencriptación.

La aplicación más inmediata de un algoritmo de encriptación (aunque no la única) es asegurar el servicio de confidencialidad: la información transmitida no se podrá desencriptar sin el conocimiento de la clave de desencriptación.

La seguridad de un sistema de cifrado radica casi totalmente en la privacidad de las claves secretas. Por ello, los ataques que puede realizar un criptoanalista enemigo están orientados a descubrir dichas claves.

La principal diferencia de los sistemas criptográficos modernos respecto a los clásicos está en que su seguridad no se basa en el secreto del sistema, sino en la robustez de sus operadores (algoritmos empleados) y sus protocolos (forma de usar los operadores), siendo el único secreto la clave (los operadores y protocolos son públicos).

El cifrado es, en su forma más simple, hacer ininteligible un mensaje de modo que no pueda leerse hasta que el receptor lo descifre. El emisor utiliza un patrón algorítmico o clave, para cifrar el mensaje. El receptor tiene la clave de descifrado.

Existen dos tipos de clave que pueden utilizarse para el cifrado:

- Claves simétricas.

- Claves asimétricas.

Las claves simétricas siguen un modelo antiguo en que el emisor y el receptor comparten algún tipo de patrón. Por lo tanto, el mismo patrón lo utilizan el emisor para cifrar el mensaje y el receptor para descifrarlo.

El riesgo que implican las claves simétricas es que deberá buscar un método de transporte seguro para utilizarlo cuando comparta su clave secreta con las personas con las que desea comunicarse.

Con las claves asimétricas se crea una pareja de claves. La pareja de claves está compuesta de una clave pública y una clave privada, que son distintas entre sí. La clave privada contiene una parte mayor del patrón cifrado secreto de la clave pública.

Como emisor, podrá difundir su clave pública a cualquier persona con la que desee comunicarse de forma segura. De este modo, conserva la clave privada y la protege con una contraseña.

A diferencia de las claves simétricas, la clave privada y la clave pública no son iguales. Como resultado, el mensaje que se ha cifrado con una clave pública sólo puede ser descifrado por la persona que lo ha cifrado, ya que dicha persona es el único propietario de la clave privada.

Un protocolo como el protocolo SSL (Secure Sockets Layer) utiliza tanto el cifrado de claves públicas como el cifrado de claves simétricas. El cifrado de claves públicas se utiliza para el protocolo de conexión TCP/IP. Durante el protocolo de conexión, la clave maestra se pasa del cliente al servidor. El cliente y el servidor crean sus propias claves de sesión utilizando la clave maestra. Las claves de sesión se utilizan para cifrar y descifrar los datos del resto de la sesión.

Una de las principales ventajas de la criptografía de clave pública es que ofrece un método para el desarrollo de firmas digitales.

Existen varios métodos para firmar documentos electrónicamente, variando desde los simples (por ej. insertar una imagen scaneada de una firma escrita a mano en un documento) hasta los avanzados (por ej. utilizando criptografía). Las firmas electrónicas basadas en criptografías de clave pública son llamadas *Firmas Digitales*.

La firma digital permite al receptor de un mensaje verificar la autenticidad

del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

Las firmas digitales son una solución que ofrece la criptografía para verificar:

- La integridad de documentos.
- La procedencia de documentos.

La firma digital es el equivalente a la firma manuscrita en el mundo electrónico, con la ventaja de que esta es infalsificable mientras no se descubra la clave secreta del firmante.

Una firma digital es una cadena de datos creada a partir de un mensaje, o parte de un mensaje, de forma que sea imposible que quién envía el mensaje reniegue de él (repudio) y que quien recibe el mensaje pueda asegurar que quién dice que lo ha enviado es realmente quien lo ha enviado, es decir, el receptor de un mensaje digital puede asegurar cual es el origen del mismo (autenticación). Así mismo, las firmas digitales pueden garantizar la integridad de los datos (que no se hayan modificado los datos durante la transmisión).

Sin embargo ya se ha comentado el principal inconveniente de los algoritmos de clave pública : su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar éste problema, la firma digital hace uso de funciones Hash. Una función *Hash* es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado resumen de los datos originales, de tamaño fijo e independiente el tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un mismo resumen hash.

Resulta evidente la importancia de estar realmente seguros de que la clave pública que manejamos para verificar una firma digital o cifrar un texto, pertenece realmente a quien creemos que pertenece.

Sería nefasto cifrar un texto confidencial con una clave pública de alguien, que no es nuestro intencionado receptor. Si lo hiciéramos, la persona a quién pertenece la clave pública con la que lo hemos cifrado podría conocer perfec-

tamente el contenido de este, si tuviera acceso al texto cifrado. Y nuestro intencionado receptor perdería toda posibilidad de acceder al texto cifrado.

De la misma forma si manejáramos una clave pública de alguien que se hace pasar por otro, sin poderlo detectar, podríamos tomar una firma fraudulenta por válida y creer que ha sido realizada por alguien que realmente no lo es.

De lo que se trata es de garantizar la identidad de las claves públicas, o más propiamente, asociar éstas a usuarios. Podemos resolver este problema usando técnicas de criptografía asimétrica y firma digital, aplicadas a las claves públicas y a una descripción del usuario, en vez de a los mensajes. Esto se llama certificar las claves y para ello se hace uso de un documento electrónico denominado certificado, que identifica una clave pública con su poseedor.

El conjunto de sistemas que proporcionan los servicios de cifrado y firma digital basados en la tecnología de claves públicas y los mecanismos de gestión de claves se denomina Infraestructura de Clave Pública o PKI (Public Key Infrastructure). Su objetivo es gestionar las claves y los certificados asociados de forma transparente a los usuarios. Por tanto, permite alcanzar un entorno de comunicaciones seguro sin necesidad de que los usuarios gestionen sus certificados. Y permitiendo que las organizaciones aborden el problema de la seguridad con una estructura centralizada que gestiona de forma transparente todas los certificados, para todas las aplicaciones uniformemente.

Hablamos de establecer relaciones de confianza a través de un tercero ('third-party Trust') cuando dos partes que previamente no se conocen confían la una en la otra. La confianza en esta situación nace de las relaciones que cada parte tiene con un tercero, y ese tercero responde por cada uno de ellos.

Este concepto es un requisito fundamental para las implementaciones a gran escala de sistemas de seguridad basados en tecnología de clave pública. La criptografía de clave pública requiere el acceso a las claves públicas de los usuarios. Cuando el número de usuarios es elevado es imposible e irreal que cada usuario tenga relaciones con el resto. Dentro de una PKI el agente que se encarga del rol de certificar la autenticidad de los usuarios es la Autoridad de Certificación (AC).

La AC dispone de un sistema de claves criptográficas que son usadas para crear y verificar las identidades electrónicas de los usuarios de la PKI. Específicamente la AC crea Certificados Electrónicos cuya autenticidad e integridad se garantiza a través de la firma digital creada con la clave privada de la AC. Los usuarios verifican la firma de la AC en los certificados usando la clave

pública de la AC.

Con el tiempo, una autoridad de certificación puede verse fácilmente desbordada si cubre un área geográfica muy extensa o muy poblada, por lo que a menudo delega en las llamadas Autoridades de Registro (AR) la labor de verificar la identidad de los solicitantes. Las AR pueden abrir multitud de oficinas regionales dispersas por un gran territorio, llegando hasta los usuarios en los sitios más remotos, mientras que la AC se limitaría así a certificar a todos los usuarios aceptados por las AR dependientes de ella.

Hoy en día existen innumerables programas para fines criptográficos pero uno de los más conocidos podemos decir que es el PGP son las siglas de Pretty Good Privacy. Se trata de un programa para cifrar y descifrar datos de todo tipo, y resulta especialmente práctico para el uso en correo electrónico. Algunas de sus ventajas son:

- Es un programa gratuito para usos no comerciales.
- Está disponible para múltiples tipos de ordenadores y sistemas operativos.
- Es un programa de manejo sencillo, especialmente si se usa a través de MS-DOS con un interfaz (“shell”), o en otros sistemas operativos (Windows, Mac, Linux).
- Resulta virtualmente indescifrable si la longitud de la clave es lo bastante larga.

Básicamente hablando, PGP funciona como un algoritmo del tipo de clave pública o asimétrica. En un sistema de clave pública, cada usuario crea un par de claves que consiste en una clave pública y una clave privada. Se puede cifrar un mensaje con la clave pública y descifrarlo con la privada (no se puede cifrar y descifrar con la misma clave). El usuario difunde la clave pública, poniéndola a disposición de cualquiera que quiera enviarle un mensaje. Una vez que el mensaje ha sido recibido por el usuario, éste podrá descifrarlo con su clave privada. Es evidente que la clave privada debe ser mantenida en secreto por el propietario.

Puede considerar este esquema como si fuese un buzón con dos llaves, una para abrir y otra para cerrar. Cualquiera puede introducir un mensaje en el buzón y cerrarlo, pero solamente el propietario podrá abrirlo. Una gran ventaja de este tipo de esquema criptográfico es que, al contrario que los sistemas tradicionales donde la clave de cifrado y descifrado coinciden, no es

necesario encontrar un procedimiento seguro para enviar la clave al recipiente del mensaje. [3]

También permite la opción de “firmar” un mensaje con una firma digital que nadie, ni siquiera el receptor, puede falsificar. Esto resulta especialmente útil, aunque no se cifre el mensaje en sí, porque actúa como certificación de autenticidad, ya que permite comprobar si el mensaje ha sido alterado durante la transmisión. También permite al receptor confirmar que el mensaje ha sido enviado realmente por el remitente (resulta demasiado fácil trucar los encabezamientos de los mensajes de correo electrónico).

La estructura operativa de PGP es bastante curiosa. Para cifrar los datos se emplea un algoritmo de clave simétrica, cuya clave es cifrada con un algoritmo de clave asimétrica. ¿Por qué esta mezcla?. Porque de este modo se combinan las mejores propiedades de ambos: la seguridad de un algoritmo asimétrico (donde clave pública y privada son distintas) con la rapidez y robustez de un algoritmo simétrico (cuya clave es única y, por tanto, vulnerable). Un tercer algoritmo se emplea para firmar documentos. Así, el sistema de operación de PGP (y programas similares) consta de tres subsistemas: cifrado del documento, cifrado de clave simétrica y firmado del documento

PGP, en su popular -aunque ya en desuso- versión para DOS utiliza una combinación de los más seguros algoritmos existentes en la actualidad: RSA (Rivest - Shamir - Adleman) para el cifrado de claves, IDEA (International Data Encryption Algorithm) para el cifrado del documento y MD5 (Message Digest Algorithm 5) para la creación de firmas digitales. La clave de tipo Diffie-Hellman, de reciente creación, emplea los algoritmos IDEA para el cifrado de documentos, Diffie-Hellman o DH (variante ElGamal) para el cifrado de la clave, y DSS (Digital Signature Standard) para firma digital. Las versiones modernas para Windows 9x y otros sistemas operativos permiten la elección del algoritmo para cifrado de documentos entre tres de los mejores que se conocen: IDEA, TripleDES y CAST.

En la actualidad, los usuarios pueden elegir entre variantes del programa PGP para diversos sistemas operativos. La antigua para MS-DOS, conocida como versión 2.6.3i ha sido libremente distribuida por todo el mundo y utiliza las claves RSA antedichas; aunque muy potente, es un programa que corre bajo DOS, por lo que requiere interfaces (shells). Las versiones posteriores resultan más fáciles de usar, especialmente cuando se combina con programas de correo electrónico como Eudora u Outlook. Actualmente es objeto de debate entre la comunidad criptográfica, principalmente por la adopción de claves Diffie-

Hellman (DH), de nuevo diseño.

A pesar de su obsolescencia, la versión para MS-DOS tiene aún numerosos partidarios. Las versiones nuevas para Window/Mac/otros son más sencillas de manejar, pero ocupan una cantidad respetable de espacio en disco duro. Por contra, la 2.6.3i funciona bajo DOS y es de tamaño reducido (cabe ampliamente en un disquete), pero es preciso, bien utilizar un interfaz adicional, bien aprender engorrosos códigos de operación. Otra diferencia consiste en el tipo de claves utilizadas. Las versiones nuevas incorporan la posibilidad de generar y utilizar tanto las viejas claves RSA como las nuevas Diffie-Hellman (DH), mientras que la 2.6.3i utiliza solamente las RSA. Usted elige.

El programa pregunta entre otras cosas:

a) Tamaño de la clave. Se recomienda 1.024 o 2.048 bits, si bien puede elegir el tamaño que prefiera. Como regla de andar por casa considere lo siguiente: el ordenador más rápido del mundo en la actualidad necesitaría una semana para romper una clave de 512 bits, 150 años para romper una de 768 bits y unos 200.000 años para violentar una clave de 1024 bits (no está mal para un programa criptográfico que cabe en un disquete). Máquinas con hardware especialmente diseñado para romper claves pueden tardar bastante menos, pero aún así nos movemos en las escalas de muchos años.

b) Identificación del usuario. Se suele usar el nombre seguido de la dirección electrónica, p. ej. “Juan Jiménez < jjimenez@virtual.serv.es >” (Aunque puede ud. identificarse como prefiera, la combinación Nombre + email suele ser la más utilizada).

c) Contraseña. Se trata de una frase clave que se deberá entrar cada vez que quiera cambiar las características de su clave secreta o, simplemente, usarla. No necesita ser una sola palabra, sino una frase fácil de recordar, como “Curro se va al Caribe” (recuerde que hay diferencia entre mayúsculas y minúsculas). Esta contraseña no debe ser divulgada *nunca* y bajo ninguna circunstancia.

d) Random bytes. Se le pedirá que teclee durante unos segundos. El propósito de ello es el de dotar al generador de claves con una ristra de bits elegidos al azar; en este caso, los bits provienen de los intervalos entre la pulsación de una tecla y la siguiente. Por ello, teclee múltiples teclas a diversas velocidades.

Hecho esto, el programa creará dos ficheros: pubring.gpg (donde se guardará su clave pública, junto con otras claves de otros usuarios que vaya ud.

recogiendo en el futuro) y `secring.pgp` (que contiene su clave secreta). Es extremadamente importante que mantenga `secring.pgp` bajo siete llaves. Cuando ud. quiera distribuir su clave pública para que le envíen mensajes cifrados, solamente ha de teclear `PGP -kxa e-mail archivo.txt` (donde “e-mail” es su dirección de correo electrónico y `archivo.txt` es el nombre del archivo que contiene su clave pública).

Con las versiones para otros sistemas operativos, el proceso es más sencillo. Solamente ha de ejecutar `PGPkeys` y activar la opción `keys/new key` (claves/nueva). El programa le dará las instrucciones a seguir. Los ficheros que contienen las claves se llaman en este caso `pubring.pkr` y `secring.skr`.

Un último detalle: en ambos casos debe firmar inmediatamente su propia clave pública. De otro modo, un usuario sin escrúpulos puede alterarla para hacerla pasar por propia. Use el comando `-ks` si usa la versión 2.6.3i; la 5.5.3i y posteriores firma automáticamente las claves creadas.

Si quiere utilizar el programa PGP, necesitará conocer todos sus comandos. Puede obtenerlos tecleando “`PGP -h`”. Sin embargo, activar los diversos comandos es una labor frustrante e ingrata, con el engorro añadido de tener que salir constantemente al sistema operativo DOS.

Es por esto que, en vez de tal cosa, se suele operar con PGP por intermedio de un programa de interfaz (“shell”) desde Windows, que convierte los códigos de uso en simples botones dentro de un programa Windows. Existen muchos de estos programas en circulación. ¿Cuál utilizar?. Los shells que se mencionarán no son necesariamente los mejores o los más eficaces, sino que han sido seleccionados de entre muchos. Se debe tener en cuenta la situación legal de estos programas. Aunque son de libre distribución, algunos requieren un registro y el pago de derechos a los autores.

Uno de los problemas más importantes acerca del esquema de criptografía de clave pública (cualquiera que sea la versión utilizada) es la autenticación, esto es, ¿Cómo saber si la clave pública realmente pertenece a quien afirma?.

Aclaremos este punto con un ejemplo. Alicia quiere enviar un mensaje a Benito. Para ello, recibe la clave pública de Benito y con ella cifra un mensaje para enviárselo. Desafortunadamente, otro usuario (llamémosle Carlos) ha generado un par de claves pública-privada y ha ubicado su propia clave pública afirmando que es la de Benito. Alicia, sin saberlo, cifra el mensaje; pero, puesto que la clave realmente pertenece a Carlos, es éste quien podrá descifrar el mensaje más tarde. Es como si Carlos crease un buzón de correos rotulado

“Benito” pero que realmente no pertenece a Benito.

¿Cómo se puede evitar esta usurpación de personalidad?. Debemos asegurarnos de que la clave de Benito no ha sido manipulada o creada por otro. Para ello, no debemos fiarnos de claves públicas transmitidas por un tercero u obtenidas en lugares dudosos (por ejemplo, un BBS, o Servicio Electrónico de Tableros). La mejor forma es pedírsela al propio Benito, bien personalmente, bien accediendo a direcciones electrónicas (http, ftp, correo-e) que sepamos pertenecen a Benito y se encuentran bajo su control; también podemos ponernos en contacto con él para que pueda verificar que la clave que poseemos realmente es suya.

Puesto que no siempre es esto posible, también existe la posibilidad de aceptar una clave si viene avalada por una persona de nuestra confianza. Esto se puede lograr mediante la firma de claves. Cualquier clave pública puede ser “firmada” digitalmente por terceros, los cuales dan fe de la autenticidad de esa clave. Si, por ejemplo, usted tiene confianza en Diego, una clave pública firmada por él será para vd. garantía de la veracidad de la clave pública por usted conseguida. Lo mismo sucede al revés: si su clave pública ha sido firmada por otros usuarios, cualquier persona que confíe en ellos aceptará su clave.

El proceso se puede jerarquizar, de tal modo que existen Autoridades de Certificación (AC) centrales para claves PGP; así, podríamos fiarnos de una AC gubernamental del mismo modo que confiamos en un documento emitido por el Estado (DNI, pasaporte, libro de familia). Alternativamente, una AC puede actuar como un servidor de claves: una especie de listín telefónico, donde se guardan claves públicas de muchas personas. Puede así obtenerse la clave pública de una persona, o bien comprobar que una clave obtenida por otros medios es auténtica (análogamente a como obtenemos y verificamos números de teléfono en las páginas amarillas).

En la actualidad, la tendencia es a que las AC sean empresas privadas (por ejemplo, VeriSign, Thawte o la española IPS), en tanto que los servidores de claves son entidades no lucrativas. Como ejemplo, he aquí el Servidor de claves de RedIris.

En cualquier caso, PGP le proporcionará cifrado seguro si sigue normas de seguridad sencillas y básicas:

1. Utilice solamente claves públicas de confianza; no se fíe de claves trans-

mitidas por terceros, por conductos inseguros o que no son verificables. Juzgue la validez de una clave en función de las firmas que la avalan. Y viceversa: procure que las personas que vayan a enviarles mensaje cifrados tengan acceso a su clave pública, y que ésta este adecuadamente avalada por terceros de confianza.

2. Mantenga el control físico sobre su anillo de claves públicas (pubring). El objetivo es protegerlo contra manipulación, no contra exposición. Guarde cuidadosamente el fichero de clave secreta (secring) contra cualquier tipo de uso por parte de terceros. Y conserve una copia de seguridad de ambos ficheros (pubring y secring).
3. *Nunca* firme una clave pública de otra persona a no ser que esté realmente seguro sobre la identidad del propietario.
4. Tampoco firme documentos que le presenten al azar; no sólo pondría su credibilidad en juego, sino que un fisgón podría utilizar esa información para intentar violentar su clave.

Con estas sencillas precauciones (sentido común, al fin y al cabo), su herramienta de cifrado será totalmente segura.

Capítulo 2

Seguridad Informática

Para comenzar a hablar de criptografía y sistemas criptográficos primero debemos tener bien en claro que es la seguridad. [7]

2.1 Definición

Se entiende por seguridad de los sistemas de información al conjunto de recursos (metodologías, planes, políticas documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

- Confidencialidad:

Se define como la “condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados”. La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. A menudo se la relaciona con la Intimidad o Privacidad, cuando esa Información se refiere a personas físicas.

- Integridad:

Se define como “la condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado”. La integridad está vinculada a la fiabilidad funcional del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél). La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

- Control:

Permite asegurar que sólo los usuarios autorizados puedan decidir cuando y como permitir el acceso a la misma.

- Disponibilidad:

Se define como el “grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable”. Se asocia a menudo a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información. La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o “tirar” el servidor.

- Autenticación:

Se define como “el mecanismo que permite conocer si la persona que esta accediendo a un sistema, es realmente quien debe acceder y no un extraño”. El no repudio se refiere a los que se hacen sobre en temas de correo electrónico para garantizar la autenticidad del remitente (un mecanismo son las firmas digitales).

Adicionalmente pueden considerarse aspectos adicionales relacionados pero que incorporan aspectos particulares:

- Protección a la réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples del mismo remitente original.
- No repudio: mediante la cual se evita que cualquier entidad que envió o recibió información niegue, ante terceros, que la envió o recibió.
- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- Aislamiento: este aspecto, íntimamente relacionado con la confidencialidad permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- Auditoria: es la capacidad de determinar que acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

2.1.1 Análisis del objetivo de la seguridad informática [1]

Para comenzar el análisis de la seguridad informática se deberá conocer las características de lo que se pretende proteger: la información.

Definimos *Dato* como la unidad mínima con la que se compone cierta información (Datum = a lo que se da).

La *información* es una agregación de datos que tiene un significado específico más allá de cada uno de estos, y tendrá un sentido particular según como y quién la procese.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe información que debe o puede ser pública (puede ser visualizada por cualquier persona), y aquella que debe ser privada (sólo puede ser visualizada por un grupo selecto de personas que trabajan con ella). En esta última

debemos maximizar los esfuerzos para preservarla de ese modo reconociendo las siguientes características en la información:

- Es crítica :es indispensable para garantizar la continuidad operativa.
- Es valiosa:es un activo con valor en si mismo.
- Es sensitiva:debe ser conocida por las personas que la procesan y sólo por ellas.

2.1.2 Principios básicos para la seguridad

- Suponer que el diseño del sistema es público.
- El defecto debe ser: sin acceso.
- Chequear permanentemente.
- Los mecanismos de protección deben ser simples, uniformes y construidos en las capas más básicas del sistema.
- Los mecanismos deben ser aceptados sicológicamente por los usuarios.

Requisitos

Los requisitos en seguridad de la información dentro de una organización sufren continuamente muchos cambios. Antes que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información, que era de valor para una institución se conseguía fundamentalmente por medio físicos y administrativos. Como por ejemplo el uso de caja de seguridad con combinaciones de apertura para almacenar documentos confidenciales.

Con la introducción de las computadoras, fue evidente la necesidad de herramientas automáticas para proteger los ficheros y otras informaciones almacenadas en su memorias.

Uno de los problemas que afecta a la seguridad, es la introducción de los sistemas distribuidos y la utilización de redes y facilidades de comunicación para transportar datos entre terminales de usuarios y computadoras, y de computador a computador. Así como también el enorme crecimiento que ha tenido Internet en la última década.

Como ya mencionamos se la debe considerar a la seguridad como un aspecto de gran importancia en cualquier organización que trabaje con sistemas informáticos.

2.1.3 La seguridad como problema cultural

Una de las paradojas es que a pesar de que cada vez se destinan mayores recursos para el área informática y que esta se ha vuelto esencial para la gestión de negocios de las empresas, el presupuesto asignado específicamente al tema de seguridad, no ha crecido en la misma proporción. Por esto es fundamental crear conciencia al interior de las organizaciones para que puedan dimensionar en su justa medida la relevancia del problema, porque si se miran los presupuestos de informática dentro de las empresas, vemos que han crecido notablemente, pero no ha ocurrido lo mismo con los presupuestos asignados a las áreas de seguridad.

Mientras más tecnología se incorpora, mas se agranda la brecha en lo que son debilidades de seguridad. Actualmente hay empresas que basan sus procesos en de negocios en TI y eso provoca que la empresa este dependiendo cada vez mas de estas herramientas tecnológicas y paralelamente van creciendo los temas relacionados con la seguridad. Por esto es fundamental la creación de conciencia en las empresas.

Una de las razones por las cuales no ha despegado fuertemente el comercio electrónico en el país es que ante la decisión de las empresas de abrirse a este tema, que va a requerir el desarrollo de mecanismo de seguridad, prefieren postergarla y si ha este le sumamos la precaria condición de la legislación con respecto al tema la opción queda desechada.

La tecnología disponible hoy en día hace posible una transferencia electrónica en forma segura, el problema es que la gente no sabe como hacerlo y tiene como consecuencia que el país se esta quedando atrás no por un problema tecnológico, si no por un problema de mentalidad. Sin duda como vemos la seguridad es fundamental no solo para evitar desastres o perdidas irrecuperables que afecten el funcionamiento de las organizaciones, sino que también para potenciar nuevas áreas de negocios que permitan el crecimiento de los diferentes actores del mercado.

2.1.4 La seguridad como proceso

Uno de los puntos de consenso en el tema es que la seguridad es un proceso y no actividad particular que desarrolla la empresa, un proceso que barre todas las unidades funcionales de esta. Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no solo implica una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar confiabilidad a la información, lo que en ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.

El problema hay que enfrentarlo con tecnología, pero también debe involucrar a los tomadores de decisiones, que son finalmente quienes deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

2.1.5 Factores que afectan a los sistemas de información

Los principales factores que se ciernen sobre los sistemas Informáticos tienen orígenes diversos. Así, si consideramos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, terremotos, sabotajes,... Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos intensos y frecuentemente, por errores de operación. Las líneas de comunicación pueden ser interferidas, etc.

Otros tipos de amenazas provienen de usuarios o empleados infieles. Así, los primeros pueden usurpar la personalidad de usuarios autorizados y acceder indebidamente a datos para su consulta o borrado, o aunque algo más complicado, modificar en su provecho programas de aplicación.

Otras amenazas más sutiles provienen de inadecuados controles de programación. Así, el problema de residuos, es decir, de la permanencia de información en memoria principal cuando ésta es liberada por un usuario o, en el caso de dispositivos externos cuando ésta es incorrectamente borrada.

Una técnica fraudulenta muy usada consiste en transferir información de un programa a otro mediante canales ilícitos y no convencionales (canales ocultos). En la Fig. 2.1 de la Pág22 vemos las amenazas más frecuentes a la

seguridad de un Sistema de información.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

- La prevención (antes): mecanismos que aumentan la seguridad o fiabilidad de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
- La detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
- La recuperación (después): Mecanismos que se aplican, cuando la violación de un sistema ya se ha detectado, para retornar este a su funcionamiento normal. Por ejemplo recuperación desde las normas de seguridad (backup) realizadas.

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc. La seguridad de la misma será nula si no se ha previsto como combatir un incendio.

2.2 Seguridad Física

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

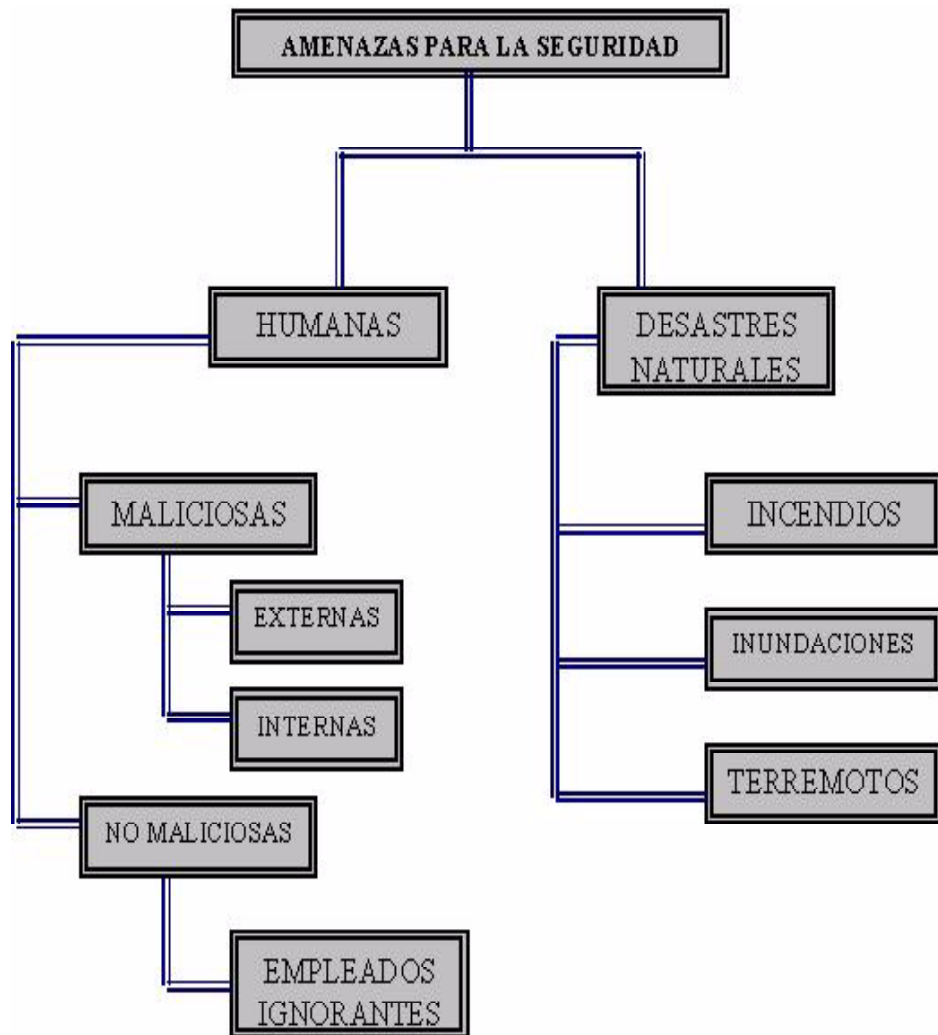


Figura 2.1: Amenazas Frecuentes.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

Los peligros más importantes que se corren en un centro de procesamiento son Incendios, inundaciones, condiciones climatológicas. El objetivo es mantener una serie de acciones para seguirlas en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección frente a estos tipos de riesgos.

2.3 Seguridad Lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo”.

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

2.4 Vulnerar para proteger

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder

colarse en ella. El trabajo de los Administradores y Testers no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.) un administrador lo hace para poder mejorar los sistemas de seguridad.

En palabras de Julio C. Ardita¹: “(...) los intrusos cuentan con grandes herramientas como los scanners, los cracking de passwords, software de análisis de vulnerabilidades y los exploits(...) un administrador cuenta con todas ellas empleadas para bien, los logs, los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones”.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa. El software y el Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina “políticas de seguridad internas” que cada organización (y usuario) debe generar e implementar.

2.5 Controles de acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

2.5.1 Acceso - Uso - Autorización

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras. Específicamente “Acceso” y “Hacer Uso” no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

- Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.
- Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.

Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario). Luego un Ataque será un intento de acceso, o uso desautorizado de un recurso, sea

satisfactorio o no. Un Incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

2.5.2 Identificación de las amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- Data Corruption: la información que no contenía defectos pasa a tenerlos.
- Denial of Service (DoS): servicios que deberían estar disponibles no lo están.
- Leakage: los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

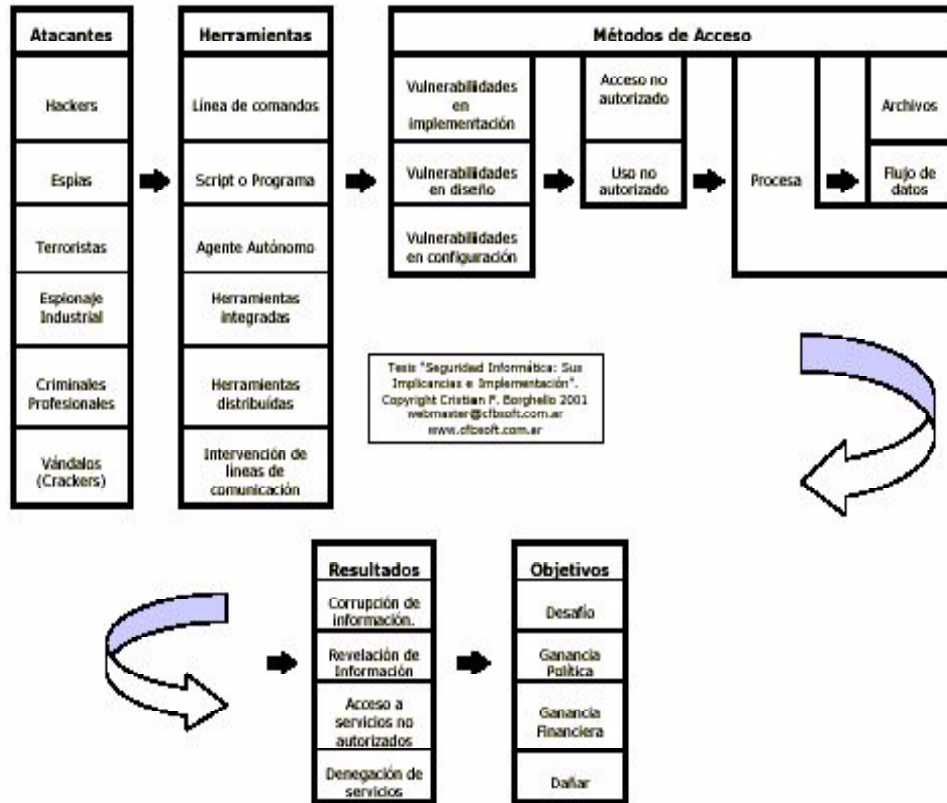


Figura 2.2: Tipos de atacantes.

La siguiente Fig. 2.2 perteneciente a la Pág. 27 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/o obtenidos y los objetivos perseguidos por los intrusos.

Cualquier persona, sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Los números que siguen no pretenden alarmar a nadie ni sembrar la semi-

lla del futuro Hacker. Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

2.5.3 Delito Informático

Ya hemos dejado en claro la importancia de la información en el mundo altamente tecnificado de hoy. También se ha dejado en claro cada uno de los riesgos “naturales” con los que se enfrenta nuestro conocimiento y la forma de enfrentarlos.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

2.5.4 Riesgos “No naturales”

Son aquellos que se encuadran en el marco del delito. El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: “no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún”.

En 1983, la Organización e Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano inter-

nacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburg (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el “principio de subsidiariedad”.

Se entiende Delito como: “la acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas”. Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos”.

“Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma”.

2.5.5 Estrategias de seguridad

El diseñar una estrategia de seguridad depende en general de la actividad que se desarrolla, sin embargo se pueden considerar tres pasos generales:

1- Crear una política global de seguridad: se debe establecer el status de la información para la empresa u organización, debe de contener un objetivo general, la importancia de la tecnología para la empresa, el periodo de tiempo de validez de la política, los recursos con que se cuentan y los objetivos específicos de la empresa. Además debe establecerse la calidad de la información a manejar según el objetivo, es decir que se establezca cuando o para quien la información debe ser confidencial, cuando debe verificarse su integridad, su autenticidad, tanto de la información como de los usuarios. [6]

2 - Realizar un análisis de riesgo: enumerar todo tipo de riesgos a los cuales esta expuesta la información y cuales son las consecuencias, los posibles atacantes, amenazas, etc.

3 - Aplicar las medidas correspondientes de seguridad: esto se puede plan-

tear como la terminación de toda la estructura de seguridad de la información. Una vez planteada la política, es decir cuanto vale la información (en un análisis de riesgo), decir que tanto se pierde si le pasa algo a la información o que tanto se gana si esta protegida, debemos de establecer las medidas para que cumpliendo con las políticas las pérdidas sean las menores posibles.

Las posibles medidas a establecer se pueden dividir en:

Tipo	Preventivas	Detectivas	Correctivas
Protección Física	PF	DF	CF
Medidas Técnicas	PT	DT	CT
Medidas de Organización	PO	DO	CO

Donde :

PF podría ser el control en el acceso de entrada, protección al hardware, respaldo de datos;

DF podría ser detectores de movimiento, de metales, monitores de vigilancia,...

CF podría ser respaldos de fuente de poder;

PT firewalls, criptografía, bitácora;

DT control de acceso lógico, sesión de autenticación;

CT programas antivirus;

PO podría ser organizaciones en las claves de acceso;

DO monitoreos de auditoria y finalmente plan de incidentes, respaldos automáticos correspondientes a CO.

En cuanto a las políticas de seguridad hoy es imposible hablar de un sistema cien por cien seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La RFC 1244 define Política de Seguridad como: “una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán”.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, “(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas”.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. “Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares”. La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Corrientes, técnicas de seguridad ante terremotos; pero sí será de máxima utilidad en Los Ángeles, EE.UU.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Está lejos proponer un documento estableciendo lo que debe hacer un

usuario o una organización para lograr la mayor Seguridad Informática posible. Sí está dentro de las posibilidades proponer los lineamientos generales que se deben seguir para lograr (si así se pretendiese) un documento con estas características.

Esto adquiere mayor importancia aún cuando el tema abordado por estas políticas es la Seguridad Informática. Extensos manuales explicando como debe protegerse una computadora o una red con un simple Firewall, un programa antivirus o un monitor de sucesos. Falacias altamente remuneradas que ofrecen la mayor “Protección” del mundo.

En definitiva la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.

2.5.6 Otras medidas de seguridad

Mecanismos de autorización

Un sistema de computación puede verse como una colección de objetos (procesos, procesadores, segmentos de memoria, discos, impresoras, archivos, semáforos). Cada objeto debe tener un nombre único para poder identificarlo, y un número finito de operaciones que los procesos pueden efectuar sobre él (leer y escribir en archivos, P y V en semáforos). Podemos ver a estos objetos como tipos abstractos de datos.

Obviamente, un proceso no debe poder acceder objetos sobre los que no tenga autorización. También debe ser posible restringir el uso de un objeto por parte de un proceso sólo a ciertas operaciones. Por ejemplo, un proceso podría tener autorización para leer, pero no para escribir un determinado archivo.

Dominios de protección

Un dominio de protección es un conjunto de pares (objeto, operaciones); cada par identifica un objeto y las operaciones permitidas sobre él.

En cada instante, cada proceso ejecuta dentro de un dominio de protección. Los procesos pueden cambiar de un dominio a otro en el tiempo; el cómo

depende mucho del sistema. En UNIX, se asocia un dominio a cada usuario; dado un usuario y el grupo al cual pertenece, se puede construir una lista de todos los objetos que puede acceder y con qué operaciones. Cuando un usuario ejecuta un programa almacenado en un archivo de propiedad de otro usuario B, el proceso puede ejecutar dentro del dominio de protección de A o B, dependiendo del bit de dominio o *setuserid* bit del archivo.

Este mecanismo se usa con algunos utilitarios. Por ejemplo, el programa `passwd` debe tener privilegios que un usuario común no tiene, para poder modificar el archivo donde se guardan las claves. Lo que se hace es que el archivo `/bin/passwd` que contiene el programa es propiedad del superusuario, y tiene el *setuserid* encendido. Este esquema es peligroso: un proceso puede pasar de un estado en que tiene poco poder a otro en que tiene poder absoluto (no hay términos medios). Cualquier error en un programa como `passwd` puede significar un gran hoyo en la seguridad del sistema. Cuando se hace una llamada al sistema también se produce un cambio de dominio, puesto que la llamada se ejecuta en modo protegido.

Matriz de acceso

Ahora bien, ¿Cómo se las arregla el sistema para llevar la cuenta de quién puede acceder qué objetos y con qué operaciones?. Conceptualmente al menos, podemos ver este modelo de protección como una gran matriz de acceso.

Los cambios de dominio que un proceso puede hacer también podemos integrarlos a la matriz, tratando a los dominios como otros objetos, con una operación: entrar.

Una política de protección involucra decidir cómo se va a llenar esta matriz. Normalmente el usuario que crea un objeto es quién decide cómo se va a llenar la columna de la matriz correspondiente a ese objeto. La matriz de acceso es suficientemente general como para apoyar diversas políticas. Por ejemplo: La capacidad para copiar o transferir un derecho de un objeto a otro dominio.

Capacidad de un dominio para modificar los derechos en otros dominios (todos, o para un recurso específico).

El problema es cómo almacenar esta matriz. Como es una matriz poco densa (muchos de los elementos son vacíos), no resulta práctico representarla como matriz propiamente. Podríamos usar una tabla con triples (dominio,

objeto, derechos). Si un proceso dentro de un dominio D intenta efectuar una operación M sobre un objeto O , se busca (D, O, C) , y se verifica si M pertenece a C . De todas maneras, la tabla es grande, y el esquema no es muy eficiente. Además, si un objeto puede ser, por ejemplo, leído por todo el mundo, debe tener entradas para cada dominio.

Listas de acceso

Alternativamente, podemos guardar la matriz por columnas (descartando las entradas vacías). Es decir, a cada objeto se le asocia una lista de pares (dominio, derechos). Es lo que se conoce como lista de acceso o ACL. Si pensamos en archivos de Unix, podemos almacenar esta lista en el nodo- i de cada archivo, y sería algo así como

((Juan, *, RW), (Pedro, Profes, RW), (*, Profes, R))

En la práctica, se usa un esquema más simple (y menos poderoso), pero que puede considerarse aún una lista de accesos, reducida a 9 bits. 3 para el dueño (RWX), 3 para el grupo, y 3 para el resto del mundo.

Windows NT usa listas de accesos con todo el nivel de detalle que uno quiera: para cualquier usuario o grupo, se puede especificar cualquier subconjunto de derechos para un archivo, de entre {RWDPO}.

CAPACIDADES

La otra posibilidad es almacenar la matriz por filas. En este caso, a cada proceso se le asocia una lista de capacidades. Cada capacidad corresponde a un objeto más las operaciones permitidas.

Cuando se usan capacidades, lo usual es que, para efectuar una operación M sobre un objeto O , el proceso ejecute la operación especificando un puntero a la capacidad correspondiente al objeto, en vez de un puntero al objeto. La sola posesión de la capacidad por parte del proceso quiere decir que tiene los derechos que en ella se indican. Por lo tanto, obviamente, se debe evitar que los procesos puedan “falsificar” capacidades.

Una posibilidad es mantener las listas de capacidades dentro del sistema operativo, y que los procesos sólo manejen punteros a las capacidades, no

las capacidades propiamente. Otra posibilidad es cifrar las capacidades con una clave conocida por el sistema, pero no por el usuario. Este enfoque es particularmente adecuado para sistemas distribuidos, y es usado en Amoeba.

Un problema de las capacidades es que puede ser difícil revocar derechos ya entregados. En Amoeba, cada objeto tiene asociado un número al azar, grande, que también está presente en la capacidad. Cuando se presenta una capacidad, ambos números deben coincidir. De esta manera, para revocar los derechos ya otorgados, se cambia el número asociado al objeto. Problema: no se puede revocar selectivamente. Las revocaciones con ACL son más simples y más flexibles.

Mecanismos de autentificación

La autentificación, que consiste en identificar a los usuarios que entran al sistema, se puede basar en posesión (llave o tarjeta), conocimiento (clave) o en un atributo del usuario (huella digital).

Claves

El mecanismo de autentificación más ampliamente usado se basa en el uso de claves o passwords; es fácil de entender y fácil de implementar. En UNIX, existe un archivo `/etc/passwd` donde se guarda los nombres de usuarios y sus claves, cifradas mediante una función one-way F . El programa `login` pide nombre y clave, computa $F(\text{clave})$, y busca el par (nombre, $F(\text{clave})$) en el archivo.

Con claves de 7 caracteres tomados al azar de entre los 95 caracteres ASCII que se pueden digitar con cualquier teclado, entonces las 957 posibles claves deberían desincentivar cualquier intento por adivinarla. Sin embargo, una proporción demasiado grande de las claves escogidas por los usuarios son fáciles de adivinar, pues la idea es que sean también fáciles de recordar. La clave también se puede descubrir mirando (o filmando) cuando el usuario la digita, o, si el usuario hace login remoto, interviniendo la red y observando todos los paquetes que pasan por ella. Por último, además de que las claves se pueden descubrir, éstas también se pueden “compartir”, violando las reglas de seguridad. . En definitiva, el sistema no tiene ninguna garantía de que quien hizo login es realmente el usuario que se supone que es.

Identificación física

Un enfoque diferente es usar un elemento físico difícil de copiar, típicamente una tarjeta con una banda magnética. Para mayor seguridad este enfoque se suele combinar con una clave (como es el caso de los cajeros automáticos). Otra posibilidad es medir características físicas particulares del sujeto: huella digital, patrón de vasos sanguíneos de la retina, longitud de los dedos. Incluso la firma sirve.

Otros métodos de protección

1. Sistemas de detección de intrusos: son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

2. Sistemas orientados a conexión de red: monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

3. Sistemas de análisis de vulnerabilidades: analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La “desventaja” de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

4. Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido iteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.

5. Sistemas de protección a la privacidad de la información: herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pret Good Privacy (PGP), Secure Sockets Layer (SSL) y los

Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Podemos considerar que estas capas son:

1. Política de seguridad de la organización.
2. Auditoría.
3. Sistemas de seguridad a nivel de Router-Firewall.
4. Sistemas de detección de intrusos.
5. Plan de respuesta a incidentes.
6. Penetration Test.

2.5.7 Penetration Test, Ethical Hacking o prueba de vulnerabilidad

“El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos”.

El objetivo general del es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El Penetration Test se compone de dos grandes fases de testeo:

1. Penetration Test Externo: el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

- Pruebas de usuarios y la “fuerza” de sus passwords.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización .
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

2. Penetration Test Interno: este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio

2.5.8 HoneyPots, HoneyNets

Estas “Trampas de Red” son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural.

Actualmente un equipo de Honeynet Project3 trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

“Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos (...). Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los ‘fascinantes programas’ que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen”, dijo Dan Adams. “Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas”.

Esta última frase se está presentando a menudo en el tema de la investigación (y vigilancia) electrónica. Este es el caso del ex-director del proyecto Honeynet J. D. Glaser, quien renunció a su puesto después de aclarar que está convencido “que la vigilancia electrónica no es correcta, aunque se utilice en aras de la investigación (...). Ampliar un Honeynet es parecido a entrapar los derechos de otros, aunque sean los derechos de un delincuente”.

2.5.9 Firewalls

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

Un Firewall es un sistema (o conjunto de ellos) como lo vemos en la Fig. 2.3 de la Pág. 40, que está ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través

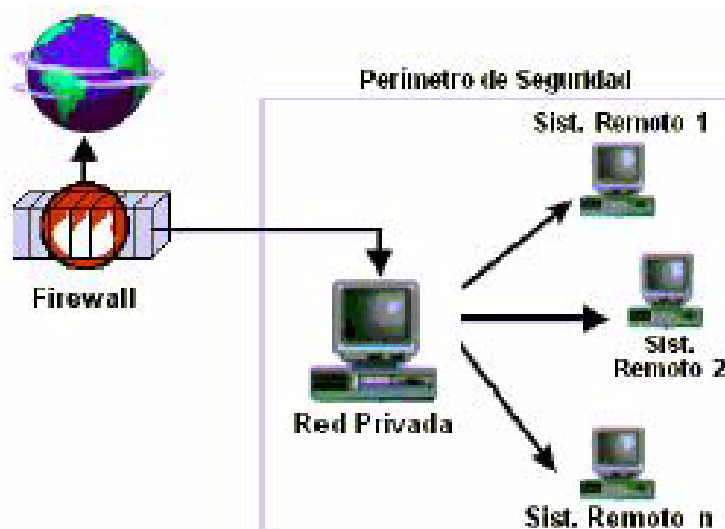


Figura 2.3: Esquema de Firewall.

de él.

2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben “hablar” el mismo método de encriptación-desencriptación para entablar la comunicación.

2.5.10 Routers y Bridges

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa.

En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace.

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo.

Los Routers “toman decisiones” en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

Algunas medidas básicas

- Demorar la respuesta ante claves erróneas; aumentar la demora cada vez. Alertar si hay demasiados intentos.
- Registrar todas las entradas. Cada vez que un usuario entra, chequear cuándo y desde dónde entró la vez anterior.
- Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo cuando usuario está de vacaciones).
- Para los más paranoicos: poner trampas para descubrir intentos de uso no autorizado.

Capítulo 3

Criptografía

Visto desde una perspectiva histórica, la necesidad de generar mensajes cifrados siempre estuvo unida a las intrigas de palacio o de la guerra. Ningún conspirador o enamorado de damas quería poner su cabeza cerca de la espada del señor del castillo cuando éste tenía una carta con pruebas en su contra en la otra mano. [?]

Entre los métodos que se creen que se usaron se encuentra uno que tiene la ventaja de ser inmune a cualquier tipo de interceptación electrónica. [8]

Primero se mandaba a llamar al cadete, que era la persona más idónea para enviar mensajes cruzando la zona de batalla. Se le cortaba el cabello y luego se le afeitaba la cabeza. Se escribía la carta sobre su cuero cabelludo, con tinta indeleble y se lo encerraba hasta que el pelo creciera nuevamente, manteniéndolo aislado de todo contacto sospechoso. Luego se lo mandaba a quien debía recibir el mensaje, quien procedía a ejecutar el mismo procedimiento, leía su misiva y en el caso que sea muy comprometedor procedía a borrar la evidencia de cualquier manera posible.

Debemos tener en cuenta que durante la primera y segunda guerra mundial transcurrió sin computadoras, la primera comenzó a funcionar recién en 1945.

Esto nos lleva a reflexionar que durante las guerras mencionadas se pueden haber propuesto algoritmos muy ingeniosos para codificar mensajes, pero para hacerlos funcionar a mano resultaba prácticamente imposible, ya fuera por el tiempo necesario o por los problemas que acarrea un error cometido en un paso intermedio.



Figura 3.1: Sistema Criptográfico.

Uno de estos algoritmos tienen su origen durante el Imperio Romano, en la época del Julio César. César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El esquema de César consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada como "M", la "B" como "N", la "C" como "O" ... así sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería el 13.

El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica". El "desplazamiento de 13 letras" es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de clave simétrica en el que se utiliza la misma clave para cifrar y descifrar el mensaje. En la fig. 3.1 de la pág.43 vemos gráficamente el concepto que introduce Julio César.

Formalmente se comenzó a hablar de la criptografía como arte hasta los trabajos de Shannon (1950), quién la relacionó con diversas disciplinas como la estadística, la teoría de los números, teorías de la información y de la complejidad. A partir de allí se la denominó ciencia.

3.0.11 Conceptos Previos

Para poder hablar de los sistemas criptográficos debemos tener una noción del vocabulario que utilizaremos:

Llamaremos "texto plano" al texto que queremos proteger mediante el uso

de técnicas criptográficas.

Llamaremos “criptograma” al texto una vez que ha sido transformado mediante alguna técnica criptográfica. Este texto resulta ilegible a no ser que se conozca la clave para volver a recuperar el “texto plano original”.

Llamaremos “encriptación” al proceso que transforma un texto plano en un criptograma.

Llamaremos “desencriptación” al proceso que recupera el texto plano de un criptograma.

3.0.12 Sistemas Criptográficos

Los sistemas criptográficos los podemos clasificar según como encripten los diferentes símbolos del alfabeto que estén utilizando.

Pueden ser *monoalféticos*, son aquellos en los que cada símbolo se encripta siempre con el mismo símbolo, la encriptación de cada símbolo es independiente del mensaje. Por ejemplo todas las “B” que aparecen en el texto plano siempre aparecen en el criptograma como “L”, esta de más aclarar que este tipo de sistemas son inseguros ya que se pueden romper mediante “análisis estadísticos de frecuencias” (se describen las características de una variable por vez, se investiga la influencia de una variable que es independiente, por vez, con respecto a la variable dependiente, se investiga la influencia de dos o mas variables independientes, junto o no a una o mas variables asociadas sobre una o más variables dependientes para representar o determinar la cantidad de veces que se presenta una variable).

A diferencia de los Monoalfabéticos, los *polialfabéticos* son aquellos en los que cada símbolo del alfabeto no se encripta con el mismo símbolo, la encriptación depende del mensaje. Por ejemplo las “B” que aparecen en el mensaje se encriptan unas veces con “L”, otras veces con “T”, otras veces con “Ñ”. De esta manera el primer requisito para que un sistema criptográfico sea seguro es que sea polialfabético.

Cuando se quiere mandar información confidencial se aplican técnicas criptográficas para poder así “esconder” el mensaje (cifrar o encriptar), luego se manda el mensaje por una supuesta línea de comunicación insegura y después sólo el receptor autorizado puede leer el mensaje “escondido” (descifrar o descencriptar). Ver la Fig. 3.2 de la Pág.45.



Figura 3.2: Comunicación Insegura.

Son muchas las técnicas criptográficas existentes y cada cierto aparecen nuevos logros y algoritmos buscando la mayor simplicidad sin minimizar la robustez de los sistemas, además existe cierta controversia que tipo de criptografía se debe utilizar. En el caso de la llamada “criptografía fuerte”, es muy segura y es prácticamente imposible descifrar mensajes encriptados con este tipo de criptografía.

La controversia surge ya que de este tipo de criptografía podría ser utilizado por organizaciones criminales para asegurar sus comunicaciones y de esta forma poder cometer sus actividades criminales de una forma más segura. Es por ello que hay interesados en que este tipo de criptografía no se utilice argumentando lo anterior, pero hay otro argumento también contundente que es el derecho a la intimidad.

Básicamente la criptografía se divide en dos ramas:

- Criptografía de Clave Privada o Simétrica.
- Criptografía de Clave Asimétrica o Pública.

Ahora bien, independientemente de si son simétricos o asimétricos, es si tiene o no estructura de grupo.

Un sistema criptográfico tiene estructura de grupo si $\forall K1, K2 \in K \exists k3 \in K$ tal que para cualquier $m \in M$ se verifica que :

$$E(E(m, K2), K1) = E(m, K3)$$

Es importante que un sistema criptográfico no tenga estructura de grupo, ya que si ciframos un mensaje con una clave K1 y luego ciframos un mensaje con otra clave K2 entonces aumentamos la seguridad del sistema. Mientras que si el sistema hubiera tenido estructura de grupo no habríamos hecho nada, ya que existiría una clave K3 que realizaría la misma operación, con lo cual no habríamos incrementado la seguridad del sistema.

3.0.13 Gestión de Claves

Todas las técnicas criptográficas dependen en última instancia de una o varias claves, por lo que su gestión es de vital importancia. Esta tarea incluye básicamente:

- La generación de las claves de forma que cumplan una serie de requisitos. Este proceso es dependiente del algoritmo en el que se va utilizar la clave en cuestión, aunque generalmente se emplea una fuente generadora de números pseudo-aleatorios como base para la creación de la clave (la clave debe ser lo más aleatoria posible).
- Registro. Las claves se han de vincular a la entidad que las usará.
- Su distribución a todas las entidades que las puedan necesitar.
- Su protección contra la revelación o sustitución no autorizadas.
- El suministro de mecanismos para informar a las entidades que las conocen en caso de que la seguridad de dichas claves haya sido comprometida (revocación).
- El tipo de método empleado para llevar a cabo la gestión de las claves es diferente según el tipo de criptografía utilizada (simétrica o asimétrica).
- Todas las claves tienen un tiempo determinado de vida, el criptoperiodo, para evitar que las técnicas de criptoanálisis tengan el suficiente tiempo e información para "romper" el algoritmo criptográfico asociado.

3.0.14 Distribución Simétrica de Claves Simétricas

Estos métodos suelen tener tres tipos de claves:

- De sesión, empleadas para encriptar los datos de usuario y que son actualizadas frecuentemente,
- De encriptación de claves, para proteger las claves de sesión, y
- Maestras, que son distribuidas manualmente y se utilizan para proteger las de encriptación de claves cuando son intercambiadas.

La distribución manual de las claves maestras es el principal inconveniente de la gestión mediante técnicas simétricas, por lo que la mayoría de los sistemas utilizan métodos asimétricos para llevar a cabo dicha distribución

3.0.15 El Acuerdo de distribución

Este método, creado por W. Diffie y M. Hellman, permite que dos entidades acuerden una clave simétrica sin necesidad de comunicación previa. El algoritmo propuesto se basa en emplear una función unidireccional con trampa (trapdoor one-way function).

Una función $y = f(x)$ se denomina unidireccional con trampa si:

- A cada valor de x le corresponde una y .
- Dado un valor de x es fácil hallar y .
- Dado un valor de y es fácil calcular x si se dispone de una cierta información (clave) y difícil sin el conocimiento de dicha información.

La función empleada por Diffie-Hellman es la exponencial discreta, cuya inversa, el algoritmo discreto es difícil de calcular.

3.0.16 Distribución Asimétrica de Claves Simétricas

Como ya se ha comentado en capítulos anteriores, el servicio de confidencialidad se puede proporcionar utilizando técnicas simétricas o asimétricas, pero estas últimas suponen una mayor carga computacional. Por ello, los métodos que se emplean comúnmente son una combinación de ambas categorías criptográficas.

Generalmente, el proceso se realiza en los siguientes pasos :

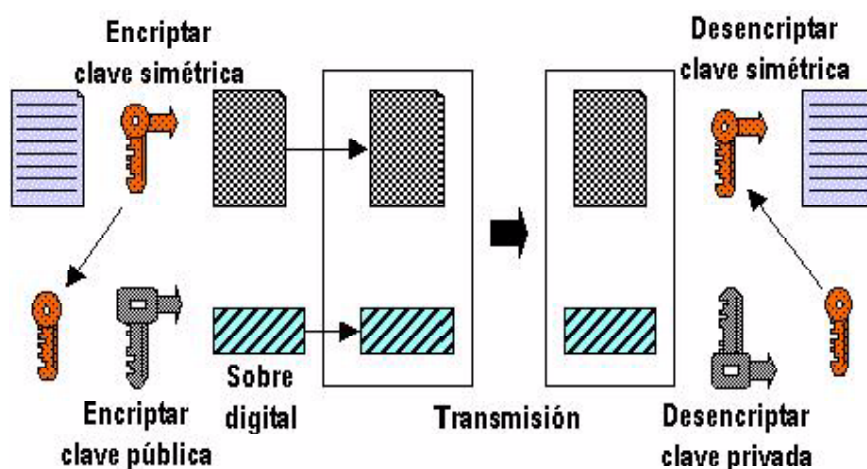


Figura 3.3: Proceso Criptográfico.

- Se encripta el texto en claro con una clave simétrica para obtener el texto cifrado.
- La clave simétrica se encripta con la clave pública del receptor obteniendo así el denominado sobre digital.
- Se envía el texto cifrado y el sobre digital.
- En recepción, se desencripta la clave simétrica con la clave privada del receptor
- Se desencripta el texto cifrado con la clave simétrica obtenida en el paso anterior para obtener el texto claro original.

En la Fig.3.3 de la Pág.48 vemos los pasos que se deben seguir para realizar el proceso criptográfico.

3.1 Criptografía Simétrica

Es el conjunto de métodos que permite una comunicación segura entre las partes componentes, siempre y cuando previamente se haya intercambiado una clave que llamaremos clave simétrica, es decir la simetría se refiere a que

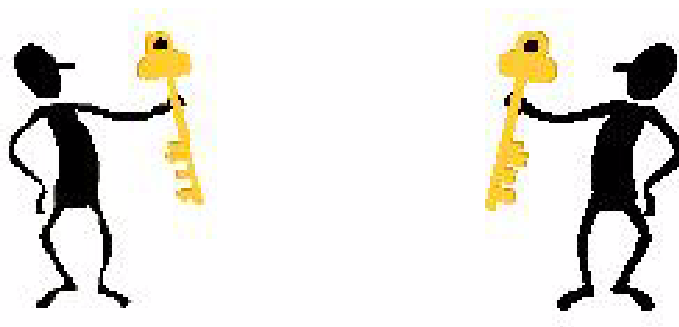


Figura 3.4: Igual Clave o LLave.

las partes usan la misma llave para cifrar, como para descifrar. Es por ello que la robustez del algoritmo recae en mantener el secreto de la misma. Su principal característica es la rapidez y facilidad de implementación. En la imagen de la Pág. ?? vemos como en este caso ambas partes utilizan la misma llave o clave tanto para cifrar como para descifrar el mensaje.

Este tipo de criptografía se la llama también criptografía de clave privada o de llave privada.

A su vez la criptografía de clave simétrica puede ser clasificada en tres grandes grupos:

- Criptografía simétrica de lluvia.
- Criptografía simétrica de bloques.
- Criptografía simétrica de resumen.

La criptografía simétrica a sido la más usada en toda la historia, se la puede implementar en distintos dispositivos, manuales, mecánicos, eléctricos, así como en los algoritmos programables en cualquier computadora. La idea general es aplicar diversas funciones al mensaje a cifrar de forma que sólo conociendo una clave se podrá descifrarlos.

Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.

Su principal desventaja es que hace falta que el emisor y el receptor compartan la clave, razón por la cual se hace inseguro el envío de la clave, ya que

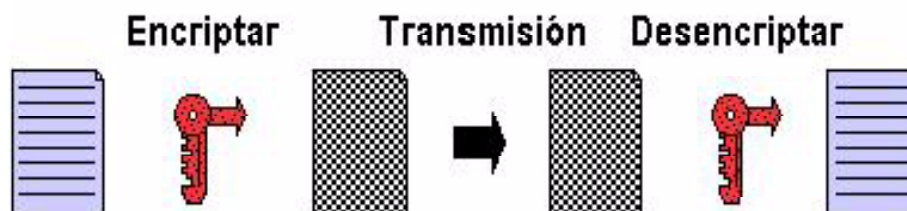


Figura 3.5: Envío inseguro de la Clave.

de cualquier forma que ésta se envíe, es posible que alguien la intercepte.

Este tipo de cifrado se utiliza para encriptar el cuerpo de los mensajes en el correo electrónico o los datos intercambiados en las comunicaciones digitales.

Para ello se emplean algoritmos como:

- DES (block, clave de 56 bits).
- 3xDES (block, clave de 112/168 bits).
- RC2 (block, Ron Rivest, reemplazo para DES, clave de tamaño variable).
- RC4 (stream, Ron Rivest).
- RC5 (block, Ron Rivest, clave arbitraria).
- IDEA (block, international data encryption algorithm. clave de 128 bits).
- NCT (block, non-linear curves traveller, clave arbitraria).

En la Fig. 3.5 de la Pág. 50 vemos como el mensaje puede ser interceptado por cualquier persona.

Otros como el cifrado de Verman verifica las condiciones de secreto perfecto definidas por Shanon, sin embargo presenta el inconveniente de que requiere un bit de clave por cada bit de texto claro. El hacer llegar tal cantidad de clave al emisor y receptor por un canal seguro desbordaría la propia capacidad del canal. Además requiere una clave aleatoria, y un ordenador genera claves pseudoaleatorias. La solución por tanto es la creación de claves de tamaño fijo y reducido.

En el caso del algoritmo DES (Data Encryption Estándar) que es el más conocido, se aplica un número finito de iteraciones de forma que da como resultado el mensaje cifrado.

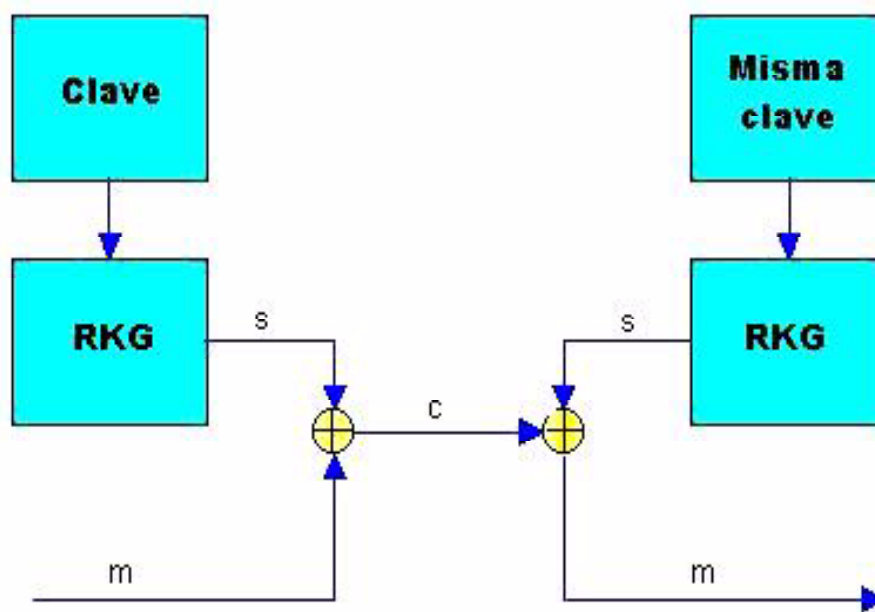


Figura 3.6: Cifrado de Flujo.

Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques. El cifrado de Flujo y el Cifrado de Bloques.

3.1.1 Cifrado de Flujo

El emisor A, con una clave secreta y un algoritmo determinístico (RKG), genera una secuencia binaria (s) cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro m, dando lugar a los bits de texto cifrado c. Esta secuencia (c) es la que se envía a través del canal. En recepción, B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante (s), que se suma modulo 2 con la secuencia cifrada (c), dando lugar a los bits de texto claro m. Los tamaños de las claves oscilan entre 120 y 250 bits. En la Fig. 3.6 de la Pág. 51 vemos gráficamente como se maneja el cifrado de flujo.

3.1.2 Cifrado en Bloque

- Los cifrados en bloque se componen de cuatro elementos:
- Transformación inicial por permutación.
- Una función criptográfica débil (no compleja) iterada r veces o “vueltas”.
- Transformación final para que las operaciones de encriptación y desencriptación sean simétricas.
- Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

3.1.3 Cifrado de Feistel

Se denominan así los criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja, alternativamente, con una de las mitades:

- Dado un bloque de N bits (típico 64) éste se dividirá en dos mitades.
- Existirá una función unidireccional F (muy difícil de invertir).

Se realizan operaciones con la clave k_i sólo con una mitad del bloque, y se permutan en cada vuelta las dos mitades, operación que se repite durante n vueltas. do un bloque de N bits (típico 64) éste se dividirá en dos mitades. En la Fig. de la Pág. vemos graficamente el cifrado mencionado.

3.1.4 El Cifrador de César

Este sistema de encriptación lo utilizaba Julio César y es un caso particular de una familia de sistemas de encriptación conocidos como “Vigenere”.

Este sistema es completamente inseguro, pero es útil para explicar los fundamentos de los métodos criptográficos. Supongamos que tenemos un alfabeto con n elementos. El método consiste en asignar un número a cada símbolo del alfabeto, $A = 0, \dots, Z = n-1$.

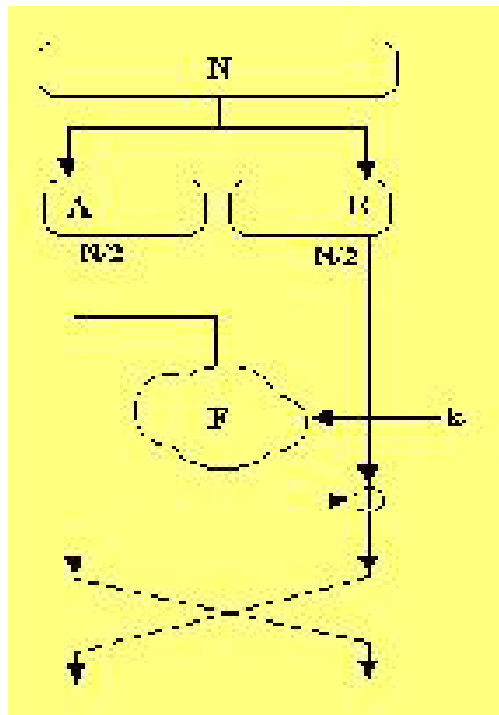


Figura 3.7: Cifrado de Feistel.

Para encriptar a cada letra le sumaremos un número, menor estrictamente, que n módulo n y le haremos corresponder la letra asociada.

Por ejemplo si nuestro alfabeto tiene 26 símbolos y elegimos como clave para encriptar 3 tendremos:

$A \rightarrow 0$ y $A+3 = 3 \rightarrow 3 \cong 3 \pmod{26}$, $3 \rightarrow D$ ya que a D le corresponde el 3.

Si para encriptar sumamos $3 \pmod{n}$, entonces para desencriptar restamos $3 \pmod{n}$. Siendo n el número de símbolos de nuestro alfabeto.

Observaciones sobre este sistema criptográfico:

Este sistema es simétrico. Las claves para encriptar y desencriptar deben mantenerse en secreto, ya que conocer una de ellas implica conocer la otra.

Este sistema es monoalfabético. Es sensible a ataques por análisis estadístico de frecuencias.

Tiene estructura de grupo, ya que si primero desplazamos m unidades cada letra, y luego lo hacemos n unidades es como si lo hubiésemos desplazado $m+n$ unidades desde el principio.

3.1.5 DES (Data Encryption Standar) [2]

Es un algoritmo desarrollado originalmente por IBM, y luego modificado y adaptado por el gobierno de los EE.UU. su nombre original era Lucifer. Trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente en hardware y en software.

A medida que fue creciendo fueron introduciéndose cambios como la reducción de la clave y de los bloques. (DES cifra bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad).

DES tiene 19 etapas diferentes. La primera es una transposición, una permutación inicial (IP) del texto plano de 64 bits, independientemente de la clave. La última etapa es otra transposición (IP⁻¹), la inversa de la primera. La penúltima etapa intercambia los 32 bits de la izquierda y los 32 de la derecha. Las 16 etapas restantes son una red de Feistel de 16 rondas.

Ahora en cada una de las 16 iteraciones se emplea un valor K_i que podemos observar como se calcula en la figura 3, obtenido a partir de la clave de 56 bits y distinto en cada iteración. Se realiza la permutación inicial (PC - 1) sobre la clave, y luego la clave obtenida se divide en dos mitades de 28 bits, cada una de las cuales se rota a izquierda un número de bits determinado que no siempre es el mismo. K_i se deriva de la elección permutada (PC-2) de 48 de los 56 bits de estas dos mitades rotadas.

La función f de la red de Feistel se compone de una permutación de expansión (E), que convierte el bloque correspondiente de 32 bits en uno de 48. después realiza una or-exclusiva con el valor K_i , también de 48 bits.

Para descifrar basta con usar el mismo algoritmo empleando. En la Fig. 3.8 de la Pág. 56 vemos gráficamente el algoritmo antes mencionado.

3.1.6 Seguridad en DES

A mediados de 1.988 se demostró que un ataque por fuerza bruta contra el algoritmo DES ya era posible, gracias al avance de la informática entre otras cosas. Pero la debilidad no la tiene el algoritmo, sino que la tiene la clave, no posee suficiente longitud la clave.

Luego si aumentamos la clave del DES este algoritmo sigue siendo seguro.

También se conocen claves débiles y semidébiles para este algoritmo, pero su número es tan pequeño en comparación con el total de claves posibles que no supone mucha preocupación.

Cuando se implantó DES en 1.977 W.DiÆe y E.Hellman analizaron una máquina capaz de encontrar la clave de cifrado en doce horas partiendo de un texto en claro y su correspondiente criptograma. Su coste era de 20 millones de dolares.

En Julio de 1.988 una empresa sin ánimo de lucro construyó una máquina que descifrababa mensajes DES en menos de tres días, el costo de este engendro era menos de 40 millones de pesetas. Pocas semanas antes un alto cargo de la NSA declaraba que DES era seguro y que descifrar mensajes DES era demasiado costoso, incluso para el gobierno .

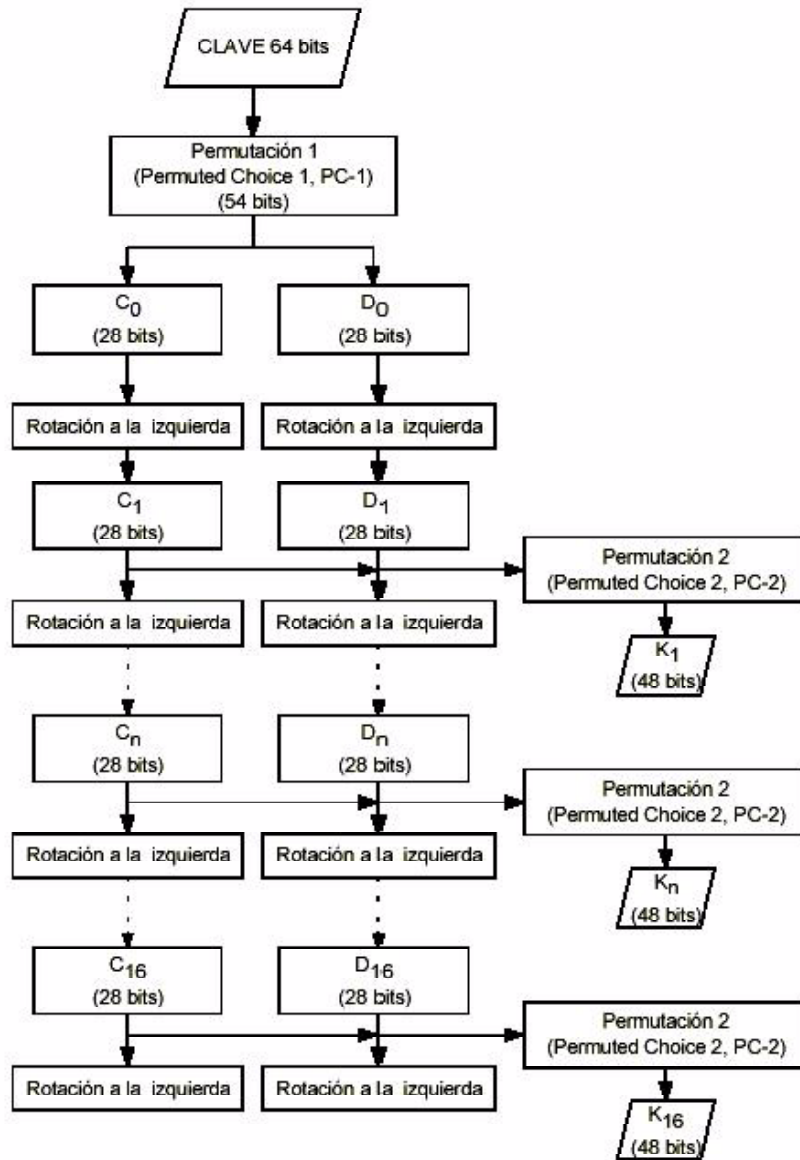


Figura 3.8: Algoritmo DES.

3.1.7 Variantes del DES

Dado al avance de la informática los ataques al DES por fuerza bruta son cada vez más fáciles y rápidos de llevar a cabo, y dado que la debilidad no reside en el algoritmo sino en la longitud de la clave los usuarios se sienten reticentes a cambiar de algoritmo.

Prefieren utilizar variantes del algoritmo y de esta forma aprovechar las implementaciones por software y hardware que existen.

3.1.8 DES Múltiple

Consiste en aplicar el algoritmo DES, con diferentes claves, varias veces. Este método aumenta la seguridad ya que el DES *no* posee estructura de grupo. Dentro de esta familia el más utilizado es el Triple-DES (3DES). Elegimos dos claves K_1 y K_2 , el procedimiento es el siguiente:

$$C = EK_1(DK_2(EK_1(M)))$$

La clave en este caso tendrá 112 bits.

Debido al actual desarrollo tecnológico, la seguridad proporcionada por una clave de sólo 56 bits de longitud está siendo cuestionada, lo que ha llevado a la búsqueda de otros sistemas simétricos alternativos como el Triple-DES que utiliza una clave de 168 bits o el IDEA que usa una clave de 128 bits.

3.1.9 IDEA (International Data Encryption Algorithm)

En este algoritmo, tanto los datos en claro como los cifrados están compuestos por bloques de 64 bits, mientras que la clave consta de 128 bits. Se basa en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes. Se realizan ocho vueltas de encriptación idénticas seguidas de una transformación de salida. Es decir, como el DES, pero las vueltas son más complejas. En cada vuelta de encriptación, el bloque de datos de entrada es dividido en cuatro sub-bloques de 16 bits. A su vez se utilizan para cada vuelta seis sub-claves.

Este algoritmo es muy seguro porque:

- Claves 2 no se pueden computar actualmente.
- No se le puede aplicar criptoanálisis diferencial a partir de la cuarta vuelta, y este tiene ocho.
- Como inconveniente tiene que si se deducen varios sub-bloques de la clave, se puede deducir la clave.

En la criptografía de clave secreta se presentan los siguientes problemas:

- Distribución de claves. Dos usuarios tienen que seleccionar una clave en secreto antes de empezar a comunicarse, lo que deberá hacer bien personalmente (cosa que no siempre es posible), bien por medio de un canal inseguro.
- Manejo de claves. En una red de n usuarios, cada pareja debe tener su clave secreta particular, lo que hace un total de $n(n-1)/2$ claves para esa red.
- Sin firma digital. En los criptosistemas de clave secreta no hay posibilidad, en general, de firmar digitalmente los mensajes, con lo que el receptor del mismo no puede estar seguro de que quien dice que le envía el mensaje sea realmente quien lo ha hecho.

3.2 Criptografía Asimétrica

Se desarrollo en los años 70' y utiliza complicados algoritmos matemáticos relacionados con números primos y curvas elípticas. En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.
- Clave pública será conocida por todos los usuarios.

Esta pareja de claves es complementaria: lo que cifra una sólo lo puede descifrar la otra y viceversa. Estas claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.

El beneficio obtenido consiste en la supresión de la necesidad del envío de la clave, siendo por lo tanto un sistema más seguro.

El inconveniente es la lentitud de la operación. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica.

Algunos algoritmos de encriptación asimétrica son:

- RSA (RIVEST-Shamir-Adelman).
- DSA (Digital Signature Algorithm).

3.2.1 RSA

Este algoritmo fue inventado por R. Rivest, A. Shamir y L. Adleman (de sus iniciales proviene el nombre del algoritmo) en el Massachusetts Institute of Technology (MIT).

RSA emplea las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo.

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable. Sin embargo, se ha de notar que, aunque el hecho de aumentar la longitud de las claves RSA no supone ninguna dificultad tecnológica, las leyes de exportación de criptografía de EE.UU. imponen un límite a dicha longitud.

El protocolo de desarrollo es el siguiente:

Cada usuario U elige dos números primos (actualmente se recomienda que tales números primos tengan más de 200 dígitos) p y q y calcula $n = p \cdot q$. El grupo a utilizar por el usuario U es, entonces, Z_n^* . El orden de este grupo es $\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$.

Después, U selecciona un entero positivo e , $1 \leq e < \varphi(n)$, de modo que sea primo con el orden del grupo, es decir, de modo que $\text{mcd}(e, \varphi(n)) = 1$.

U calcula es inverso de e en $Z_{\varphi(n)}$, d; se tiene entonces $e \bullet d \equiv 1 \pmod{\varphi(n)}$, con $1 \leq d < \varphi(n)$.

La clave pública del usuario U es la pareja (n, e) , mientras que su clave privada es el número d. Por supuesto, también deben permanecer secretos los números p, q y $\varphi(n)$.

Si un usuario A desea enviar un mensaje m de Z_n a otro usuario B, utiliza la clave pública de B, (n_b, e_b) , para calcular el valor de $m_b^e \pmod{n_b} = c$, que envía a B. Para recuperar el mensaje original, B calcula $c_b^d = (m_b^e)d_b = m_b^{ed} = m \pmod{n_b}$.

Ejemplo:

Consideremos una codificación del alfabeto que transforme las letras de la A a la Z en los números del 0 al 25 (del alfabeto inglés), y enviamos un mensaje al usuario B.

El usuario B elige dos primos $p_b=281$ y $q_b=167 \Rightarrow n_b=281 \bullet 167=46927$ y considera el grupo Z_{46927}^* .

Ahora $\varphi(46927)=280 \bullet 166=46480$ y B elige $e_b=39423$ y comprueba que $\text{mcd}(39423, 46480)=1$.

A continuación determina el inverso de 39423 módulo 46480 $\Rightarrow d_b=26767$.

Clave privada= $d_b = 26767$

Clave pública=(39423, 46927)

Para enviar un mensaje de A a B, debemos determinar en la longitud del mismo. Como el mensaje ha de ser un elemento del grupo con el que estamos trabajando, su longitud no puede exceder del valor de $n = 46927$. Así pues como $26^3=17576 < n < 456976=26^4$, el mensaje ha de tener un máximo de tres letras. Si se quiere enviar un mensaje más largo, habrá que romperlo en grupos de tres letras. En la practica, la longitud del mensaje es mucho mayor dado que n es un número con muchos dígitos.

$$\text{YES} = Y \bullet 26^2 + E \bullet 26 + S = 16346 = m$$

$$c = m_b^e \pmod{n_b} = 16346^{39423} \pmod{46927} = 21166 \text{ [valor que A envía a B]}$$

Ahora B recibe 21166 la decodificación sería así:

$$m = c_b^d \pmod{n_b} = 21166 \pmod{46927^{39423}} = 16346$$

Se decodifica m y se obtiene el texto original

$$m=16346= 24 \bullet 26^2 + 4 \bullet 26 + 18 = \text{YES}$$

El algoritmo DES implementado en software es 100 veces más rápido que RSA e implementado en chip es de 1000 a 10000 más rápido. Por tanto para mensajes cortos se debe utilizar RSA y para los largos DES.

Lo que se suele hacer es un envoltorio digital. El usuario A encripta el mensaje m con el criptosistema DES mediante una clave aleatoria, y a continuación la clave DES se encripta con RSA. Para recuperar el mensaje, el usuario B describe la clave de DES mediante su clave privada del RSA y luego utiliza la clave obtenida para descryptar el mensaje m .

Para romper RSA se necesita conocer $\varphi(n)$ del cual puede deducir d . Conocido n no es fácil determinar $\varphi(n)$ ya que $n=p \bullet q$ y no se conoce ni p ni q . Para que un RSA sea fuerte p y q tienen que ser difíciles de adivinar, esto implica que p y q sólo deben diferir en unos pocos dígitos, aunque no deben ser demasiado cercanos., $(p - 1)(q - 1)$ deben contener factores primos grandes, el $\text{mcd}(p - 1, q - 1)$ debe ser pequeño. Y una condición indispensable es que p y q sean primos.

3.2.2 Seguridad RSA

Como las claves públicas son públicas, cualquiera puede encriptar un texto a partir de un texto plano e intentar averiguar la clave privada.

Supongamos que encriptamos el texto "HOLA", durante el proceso de descryptación

tendremos:

$$45,840^d \equiv 881 \pmod{46,927}$$

$$26,074^d \equiv 381 \pmod{46,927}$$

o lo que es lo mismo:

$$d = \log_{45,840} 881 \pmod{46,927}$$

$$d = \log_{26,074} 381 \pmod{46,927}$$

d no es conocido ya que forma parte de la clave privada, para romper este

criptosistema lo podemos intentar de varias formas:

1. A fuerza bruta.
2. Mediante un ataque de intermediario.
3. Intentando resolver cualquiera de los dos logaritmos discretos anteriores . . .
4. Resolviendo: $e \bullet d \equiv 1 \pmod{\phi(46,927)}$.

Lo cual equivale a conocer $\phi(46,927)$, que a su vez equivale a conocer la factorización en números primos de 46,927.

Lo cual es un problema con el mismo grado de complejidad que el logaritmo discreto (problema de tipo exponencial) para números lo suficientemente grandes .

3.2.3 Algoritmo Asimétrico ElGamal

Supongamos que los mensajes son elementos de G y que el usuario A desea enviar un mensaje m al usuario B . El protocolo utilizado es el siguiente:

Se selecciona un grupo finito G y un elemento α de G .

Cada usuario A elige un número aleatorio a , que será su clave privada, y calcula α^a en G , que será su clave pública. Para que un usuario A envíe un mensaje, m , a otro usuario B , suponiendo que los mensajes son elementos de G , realiza las siguientes operaciones:

- A genera un número aleatorio v y calcula α^v en G .
- A mira la clave pública de B , α^b , y calcula $(\alpha^b)^v$ y $m \bullet \alpha^{bv}$ en G .
- A envía la pareja $(\alpha^v, m \bullet \alpha^{bv})$ a B .

Para recuperar el mensaje original:

- B calcula $(\alpha^v)^b$ en G .
- B obtiene m sólo con calcular $m \bullet \alpha^{bv} / \alpha^{vb}$.

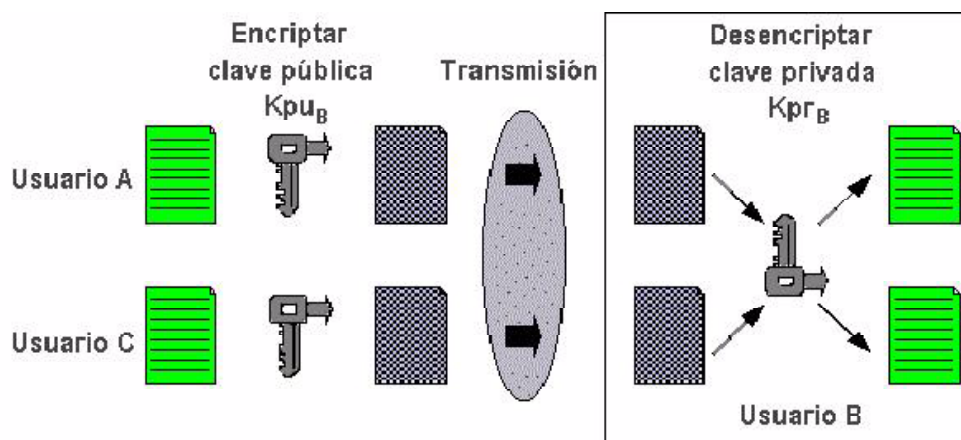


Figura 3.9: Primer Caso.

3.2.4 Digital Signature Algorithm (DSA)

Un algoritmo muy extendido es el Digital Signature Algorithm (DSA) definido en el Digital Signature Standard (DSS), el cual fue propuesto por el U.S. National Institute of Standards and Technology (NIST). Este algoritmo se basa en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible (logaritmo discreto).

3.2.5 Planteamiento de Casos

Primer caso: cuando un usuario, A, quiere enviar información a otro usuario, B, utiliza la clave pública de B (K_{puB}) para encriptar los datos. El usuario B utilizará su clave privada (que sólo él conoce) (K_{prB}) para obtener el texto en claro a partir de la información (encriptada) recibida. Si otro usuario, C, quiere enviar información al usuario B, también empleará la clave pública (K_{puB}). Este modo se puede emplear para proporcionar el servicio de confidencialidad, pues sólo el usuario B es capaz de descifrar los mensajes que los usuarios A y C le han enviado. En la Fig.3.9 de la Pág. 63 observamos gráficamente el primer caso planteado.

Segundo caso: es el usuario B quien encripta la información utilizando su clave privada, (K_{prB}) de forma que cualquiera que conozca (K_{puB}) podrá

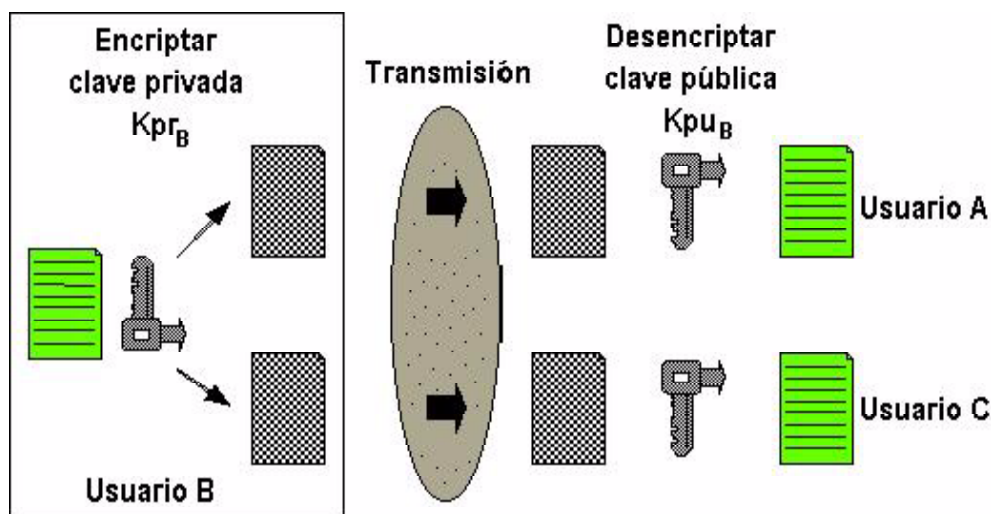


Figura 3.10: Segundo Caso.

descifrar la información transmitida. Este modo se puede emplear para proporcionar el servicio de autenticación, ya que la obtención del texto en claro a partir del texto cifrado es una garantía de que el emisor del mensaje es el propietario de (K_{puB}) (lógicamente, para saber que el mensaje obtenido de la desencriptación del texto cifrado es el texto en claro original, éste se ha de obtener por otros medios para realizar la comparación). Esto es la base de las firmas digitales. En la Fig. 3.10 de la Pág. 64 observamos gráficamente el segundo caso planteado.

Desde el punto de vista de la confidencialidad, los algoritmos asimétricos proporcionan una mayor seguridad que los simétricos a costa de una mayor carga computacional. Es por esta razón que generalmente se emplea una combinación de ambos.

En la práctica, debido a que los algoritmos de clave pública requieren mucho tiempo para cifrar documentos largos, los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen (funciones hash), de manera que en vez de firmar un documento, se firma un resumen del mismo.

Este mecanismo implica el cifrado, mediante la clave privada del emisor, del resumen de los datos, que serán transferidos junto con el mensaje. Una

vez en el receptor, éste se procesa debidamente para verificar su integridad. Por lo tanto, los pasos del protocolo son:

1. Juana genera un resumen del documento.
2. Juana cifra el resumen con su clave privada, firmando el documento. Este resumen es su firma digital.
3. Juana envía el documento junto con el resumen firmado (la firma digital) a David.
4. David genera un resumen del documento recibido, usando la misma función unidireccional de resumen.
5. Después David descifra con la clave pública de Juana, que se conoce, el resumen firmado (firma digital de Juana).
6. Si el resumen firmado coincide con el resumen que él ha generado, la firma digital es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto Juana podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por Juana, podemos estar seguros de su identidad. En último lugar, mediante la firma digital se garantiza además la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen. En la Fig.3.11 de la Pág. 66 se observa gráficamente el tercer caso planteado.

3.2.6 Funciones Hash

Como mencionamos anteriormente, el último problema que se suscita en el “viaje” de los datos, es la integridad. Si bien alguien no podrá leer lo que está viajando, ya que está encriptado, si puede modificarlo, quitándole o agregándole algunos bits, lo que puede provocar serios problemas si la información que viaja es de vital importancia.

Una Firma digital, asegura la autenticación de quien envía el mensaje, así como la integridad el mismo, ya que junto con la firma, se envía un código computado por las llamadas funciones Hash.

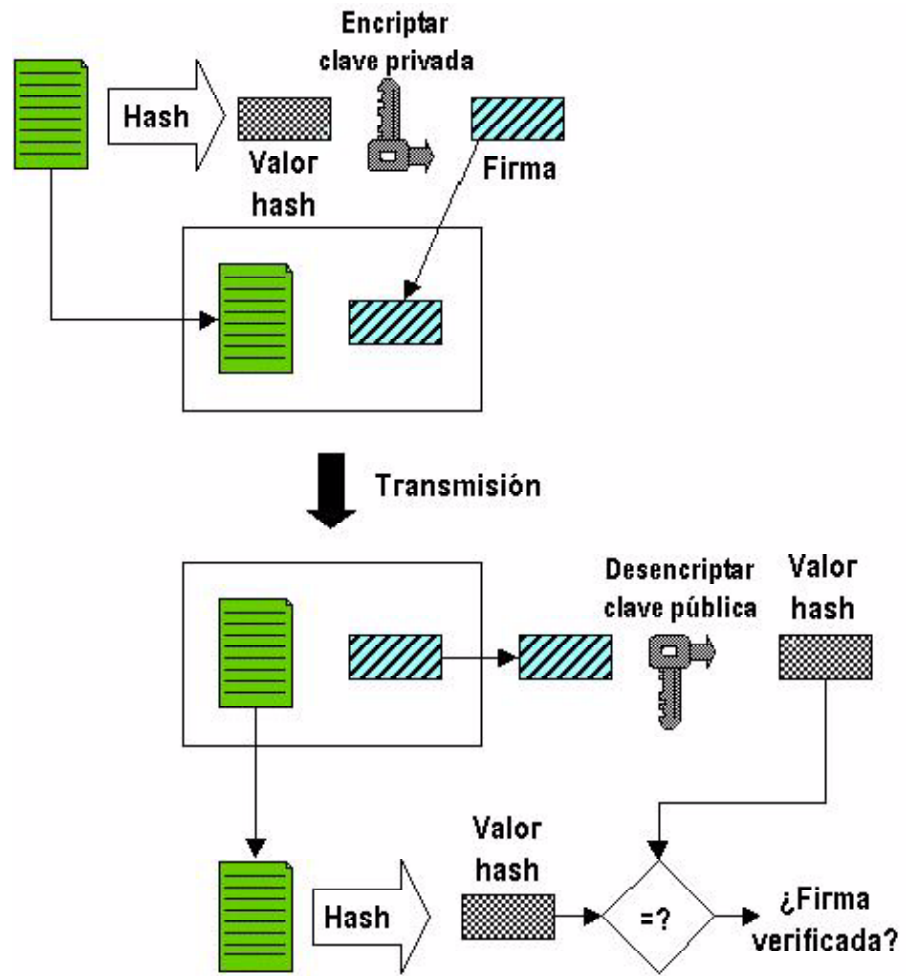


Figura 3.11: Tercer Caso.

Una Función Hash, “comprime” el mensaje, de modo de producir una especie de “resumen”, el cual será comprobado, para asegurar que se mantenga la integridad del mismo.

Se puede definir una Función Hash (función de comprobación aleatoria) como aquella que reduce el mensaje a un conjunto de datos, denominado resumen, de longitud mucho menor que el mensaje, usualmente 128 ó 254 bits y que viaja junto con el mensaje original.

La idea es que aunque obviamente hay otros mensajes que producen el mismo hash es extremadamente difícil encontrarlos y aún más difícil que tengan un significado en nuestra lengua.

Los principales Algoritmos son:

- MD2 (Message Digest-2, Ron Rivest, 128 bits, más lento, menos seguro que MD4).
- MD4 (Message Digest-4, Ron Rivest, 128 bits, muy usado).
- MD5 (Message Digest-5, Ron Rivest, 128 bits, MD4 con mejoras, muy usado, usado en SSL).
- SHA/SHA-1 (secure hash algorithm, 160 bits, usado en DSS, SSL).

Con respecto al MD5 es un algoritmo hash que toma como entrada un mensaje de una longitud arbitraria y produce un mensaje o huella digital como salida. EL MD5 es usado en firma digital cuando un gran archivo debe comprimirse en una forma segura antes de comenzar a encriptarse con una clave privada (secreta) bajo un criptosistema de clave publica como RSA.

Crea una representación numérica del contenido de un mensaje y la visualiza como valor del hexadecimal de 16 caracteres.

El SHA1 toma un mensaje de menos de 264 bits de longitud y produce una huella digital de 160 bits. Fue desarrollado por la Agencia de Seguridad Norteamericana y se considera un sistema seguro y sin fisuras.

3.2.7 Firmas Digitales

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha

sido modificada desde su generación. Las firmas digitales son una solución que ofrece la criptografía para verificar:

- La integridad de documentos.
- La procedencia de documentos.

De este modo, ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, ya que el originador de un mensaje firmado digitalmente no puede argumentar que no lo es.

Está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

Se basa en la propiedad de que un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

Pero como ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar éste problema, la firma digital hace uso de funciones hash.

Para que este tipo de funciones sean útiles, criptográficamente, deben cumplir:

- El resumen es de longitud fija.
- Calcular el resumen de un mensaje es fácil. (tiempo polinomial)

Dado un resumen es computacionalmente imposible calcular el mensaje que lo genero.

Es prácticamente imposible obtener dos mensajes que generen el mismo resumen.

Se recomienda utilizar firmas de al menos 128 bits. El tamaño más usado para firmas es de 160 bits.

Primero se produce un resumen del mensaje, luego se encripta este resumen.

Normalmente para hacer hash de un mensaje se divide en bloques y se suele incluir la longitud del mensaje original para evitar que dos mensajes de diferente longitud produzcan el mismo resumen.

Con algoritmos asimétricos nunca se debe firmar un mensaje después de encriptarlo ya que existen ataques para romper el criptosistema.

Para comprobar una firma digital se puede proceder de la siguiente forma:

- Descriptamos la firma digital, usando la clave pública si han utilizado un método asimétrico.
- Obtenemos el resumen del mensaje original.
- Hacemos un hash sobre el mensaje original.
- Comprobamos nuestro resumen con el obtenido al descriptar
- Y por último si coinciden la firma digital es válida.

3.2.8 Ventajas de la Firma Digital

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

En la vida cotidiana se presentan muchas situaciones en las que los ciudadanos deben acreditar fehacientemente su identidad, por ejemplo, a la hora de pagar las compras con una tarjeta de crédito en un establecimiento comercial, para votar en los colegios electorales, con el fin de identificarse en el mostrador de una empresa, al firmar documentos notariales, etc.

En estos casos, la identificación se realiza fundamentalmente mediante la presentación de documentos acreditativos como el DNI, el pasaporte o el carnet de conducir, que contienen una serie de datos significativos vinculados al individuo que los presenta, como:

- Nombre del titular del documento.
- Número de serie que identifica el documento.
- Período de validez: fecha de expedición y de caducidad del documento, más allá de cuyos límites éste pierde validez.
- Fotografía del titular.
- Firma manuscrita del titular.
- Otros datos demográficos, como sexo, dirección, etc.

En algunos casos en los que la autenticación de la persona resulta importante, como en el pago con tarjeta de crédito, se puede exigir incluso que estampe una firma, que será comparada con la que aparece en la tarjeta y sobre su documento de identificación. En el mundo físico se produce la verificación de la identidad de la persona comparando la fotografía del documento con su propia fisonomía y en casos especialmente delicados incluso comparando su firma manuscrita con la estampada en el documento acreditativo que porta. En otras situaciones, no se requiere el DNI o pasaporte, pero sí la firma, para que el documento goce de la validez legal (cheques, cartas, etc.), ya que ésta vincula al signatario con el documento por él firmado.

Ahora bien, en un contexto electrónico, en el que no existe contacto directo entre las partes, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de que estos últimos están dotados? La respuesta, por fortuna, es afirmativa. Se verá a continuación que el trasunto electrónico del DNI o pasaporte es el certificado digital y que el mecanismo que permite atestiguar la identidad de su portador es la firma digital.

La firma digital es el instrumento que permitirá, entre otras cosas, determinar de forma fiable si las partes que intervienen en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente. También es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este puede ser visto por otras personas.

La aplicación más inmediata que encontrarán las firmas digitales, tanto en Europa como en América, será potenciar dos importantes actividades amparadas en el seno de Internet, debido a la relación de confianza que se establece entre las partes implicadas:

En jurisdicciones de todo el mundo, las firmas digitales ganan gradualmente el mismo peso legal que la firma manuscrita. La Firma Digital es una manera segura de firmar un documento electrónico como cartas, contratos o trabajos. Brinda la garantía de que el mensaje procede en realidad del remitente, que no ha sido intervenido y que aquél es quien dice ser.

No es una firma escrita, sino un software. Se basa en algoritmos que trabajan con números de hasta 2048 bits. La parte visible de la rúbrica es el nombre del firmante, pero también puede incluir el nombre de una compañía y el cargo.

El comercio electrónico, que no termina de despegar, entre otras razones, debido al desamparo de comerciantes y consumidores ante el fraude en los modelos actuales de compra a través de Internet basados únicamente en SSL (Secure Socket Layer). Gracias a las firmas digitales se puede identificar a los participantes en las transacciones a través de Internet.

El proyecto de ventanilla única (conocido como tele administración) que pretende acercar la Administración al ciudadano, de modo que desde su propio hogar, con absoluta autonomía, utilizando su PC y conectándose a Internet, tenga la posibilidad de obtener absolutamente toda la información necesaria para la realización de cualquier trámite ofertado por las Unidades de las Administraciones Públicas; pueda igualmente descargar e imprimir cualquier tipo de formulario para iniciar la tramitación de procedimientos y expedientes administrativos; o pueda, en determinados casos elegidos, enviar los formularios correspondientes a la Administración tramitante, que le informará del estado en que se encuentra su tramitación.

3.2.9 Funcionamiento de las Firmas Digitales

Los primeros algoritmos fueron desarrollados por Whitfield Diffie y Martin Hellman en 1976. Los más populares son el RSA, de 1977 (por las iniciales de Ron Rivest, Adi Shamir y Leonard Adleman, sus inventores), incluido en el Internet Explorer y el Netscape Navigator; el DSA (por Digital Signature Algorithm, algoritmo de firma digital) del Departamento de Comercio de los

Estados Unidos, y el PGP (por Pretty Good Privacy, privacidad bastante buena, en inglés), creado en 1991 por Philip Zimmermann y usado sólo para el e-mail.

El fundamento de las firmas digitales es la criptografía, disciplina matemática que no sólo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de ojos indiscretos, sino que también proporciona mecanismos para asegurar la integridad de los datos y la identidad de los participantes en una transacción.

Todos los algoritmos se basan en un mismo método: en vez de usar una misma clave (simétrica) para encriptar y desencriptar datos (como la contraseña en un documento Word), usan dos: una privada y una pública. La primera es la que el usuario guarda; la segunda se publica en el sitio de una autoridad certificante (una entidad confiable que da fe de que la clave pública pertenece a una persona o entidad). [4]

El cifrado consiste en transformar un texto en claro mediante un algoritmo en un texto cifrado, gracias a una clave de cifrado, que resulta ininteligible para todos excepto para el legítimo destinatario del mismo.

Cada clave es el resultado de hacer ciertas operaciones matemáticas sobre dos números primos (divisibles sólo por sí mismos y por uno) muy grandes, de entre 512 y 2048 bits: los resultados son las dos claves. La importancia de usar números primos es que es extremadamente difícil factorizar las claves para recuperar los primos originales.

Para enviar un mensaje con firma digital, por ejemplo, al texto se le hace un hashing: de un texto se genera un número más chico con un algoritmo, de tal forma que es casi imposible que de otro texto se cree el mismo número. Al resultado se lo encripta usando la clave privada: ésa es la firma digital, que se envía con el mensaje original.

El destinatario recibe el texto y la firma: primero hace su propio hashing del mensaje y luego, con la clave pública del emisor, desencripta la firma: si ambos mensajes son iguales, significa que el remitente es válido y que el mensaje no sufrió alteraciones en el trayecto de un lugar al otro. Todo este proceso es invisible para el usuario; la firma digital aparece como una cadena de caracteres.

3.2.10 Seguridad de la Firma Digital

La firma digital proporciona un amplio abanico de servicios de seguridad:

- Autenticación: permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, bien para garantizar el acceso a servicios distribuidos en red.
- Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.
- Integridad: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.
- No repudio: ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un timestamp, debido a la imposibilidad de ser falsificada, testimonio que él, y solamente él, pudo haberlo firmado.
- Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,
- El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

3.2.11 Aplicación de la Firma Digital

La firma digital se puede aplicar en las siguientes situaciones:

- E-mail.

- Contratos electrónicos.
- Procesos de aplicaciones electrónicos.
- Formas de procesamiento automatizado.
- Transacciones realizadas desde financieras alejadas.
- Transferencia en sistemas electrónicos, por ejemplo si se quiere enviar un mensaje para transferir \$100,000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los \$100,000 por 1000,000 ,con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción.
- En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios.
- En sistemas legislativos, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

3.2.12 Entidades de Certificación

Ejemplo de Verisign. En los métodos asimétricos, cada entidad sólo ha de poseer un par de claves (privada y pública) independientemente del número de sistemas con los que se comunique. El único requisito que se ha de cumplir es la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo (ataque man-in-the-middle). Para evitar esto se recurre a lo que se denominan los certificados de clave pública, que son emitidos por unas entidades de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) y que garantizan que una determina clave pública pertenece a su verdadero poseedor.

Estas entidades permiten garantizar los servicios de confidencialidad e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados (Public Key Infrastructure) ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme, independientemente de las políticas de certificación empleadas.

Las CAs tienen como misión la gestión de los denominados certificados (de clave pública). Un certificado está compuesto básicamente por la identidad de un usuario (subject), su clave pública, la identidad y la clave pública de la CA emisora (issuer) del certificado en cuestión, su periodo de validez y la firma digital del propio certificado. Esta firma, realizada por la CA emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que éste contiene es auténtica (suponiendo que confíen en la CA emisora). Una vez que los certificados han sido firmados, se pueden almacenar en servidores de directorios o transmitidos por cualquier medio (seguro o no) para que estén disponibles públicamente.

Antes de enviar un mensaje encriptado mediante un método asimétrico, el emisor ha de obtener y verificar los certificados de los receptores de dicho mensaje. La validación de un certificado se realiza verificando la firma digital en él incluida mediante el empleo de la clave pública de su signatario, que a su vez ha de ser validada usando el certificado correspondiente, y así sucesivamente hasta llegar a la raíz de la jerarquía de certificación.

Por lo tanto los usuarios pueden chequear la autenticidad de las claves públicas de otros usuarios verificando la firma de la CA en el certificado usando la clave pública del CA.

En el proceso de verificación se ha de comprobar el periodo de validez de cada certificado y que ninguno de los certificados de la cadena haya sido revocado.

VeriSign es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Para el logro de este objetivo, las autoridades de emisión (Issuing Authorities, "IA") autorizadas por VeriSign funcionan como trusted third partie (o "garantes"), emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de la empresa.

Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es repre-

sentada por un certificado: un mensaje firmado digitalmente y emitido por una IA.

Esta empresa ofrece tres niveles de servicios de certificación. Cada nivel o clase de certificados provee servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades. Cumplidos los requisitos exigidos se emite el certificado.

Los Certificados Clase 1 son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indubitable el nombre del usuario o su "alias" y su dirección de E-mail con el registro llevado por VeriSign. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing e E-mail, afianzando la seguridad de sus entornos. En general, no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

Los Certificados Clase 2 son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que ella no difiere de la que surge de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía E-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones online. Debido a las limitaciones de las referidas bases de datos, esta clase de certificados está reservada a residentes en los Estados Unidos y Canadá.

Los Certificados Clase 3 son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, asegura la identidad del suscriptor, requiriendo su presencia física ante un notario. En el caso de organizaciones, asegura la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como electronic banking y Electronic Data Interchange (EDI).

Como las IAs. autorizadas por VERISIGN firman digitalmente los certificados que emiten, la empresa asegura a los usuarios que la clave privada utilizada no está comprometida, valiéndose para ello de productos de hardware. Asimismo, recomiendan que las claves privadas de los usuarios sean encriptadas vía software o conservadas en un medio físico (smart cards o PC cards).

3.2.13 Software Easy Sign

Las firmas digitales son generadas (a partir de claves asignadas a los usuarios) y verificadas por Easy*Sign, comprobando de esta manera la autenticidad e integridad del mensaje recibido y el no repudio por parte del emisor. AT&T Networked Commerce Services proveerá el Easy*Sign con funcionalidad de seguridad que estará integrado al aplicativo EDI en forma transparente para el usuario final.

Easy*Sign es un conjunto de herramientas que permiten implementar servicios de seguridad para las transacciones comerciales realizadas bajo el estándar EDIFACT de las Naciones Unidas.

Su función es la de generar los segmentos de seguridad de la firma digital y adicionarlos a la transacción que se está firmando (mediante el pedido de un password que habilita al usuario a firmar con la clave privada), además de controlar que las transacciones recibidas contengan segmentos de seguridad validadas contra la llave pública del firmante.

3.2.14 Principales funciones de la Firma

- Autenticación del originador del mensaje. RSA permite “firmar” los documentos escritos en formato “Edifact” de manera tal que el destinatario pueda validar que la información que él recibe del originador es auténtica y no la pueda negar, lográndose con esto la confianza de quien recibe el mensaje
- Autenticación del mensaje. Cuando se realiza la firma digital, previamente se calcula un valor de 160 bits (mediante el algoritmo SHA), el cual asegura al originador que si el documento sufre alguna alteración, esta va a ser detectada durante el proceso de validación de la firma.

3.2.15 Infraestructura de la Firma Digital

Esta clase de Infraestructura es también conocida como de “clave pública” o por su equivalente en inglés (Public Key Infrastructure, PKI). La normativa crea el marco regulatorio para el empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan

efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma ológrafa.

La disposición establece la configuración de la siguiente estructura:

- Organismo Licenciante (OL).
- Organismo Auditante (OA).
- Autoridad Certificada Licenciada (ACL).
- Suscriptores.

3.2.16 Organismo Licenciante

Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias del Sector Público Nacional que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.

Dentro del marco creado por el Decreto N° 427/98 , las funciones de Autoridad de Aplicación y de Organismo Licenciante son asumidas por la Subsecretaría de la Gestión Pública, SGP.

En cumplimiento de esa responsabilidad, se ha dispuesto la asignación de los recursos materiales y humanos, incluyendo la adquisición de equipamiento de última generación. Además, se ha elaborado una serie de documentos disponibles en este sitio - que se encuentran en proceso permanente de revisión - y que servirán como base para el funcionamiento de Autoridades Certificantes que se licencien.

3.2.17 Organismo Auditante

Es el órgano de control, tanto para el Organismo Licenciante como para las Autoridades Certificantes Licenciadas. Según lo establecido por el artículo 61 de la Ley N° 25.237, el rol de Organismo Auditante dentro de la Infraestructura de Firma Digital para el Sector Público Nacional es cumplido por la Sindicatura General de la Nación (SIGEN).

3.2.18 Autoridades Certificantes Licenciadas

Son aquellos organismos o dependencias del Sector Público Nacional que soliciten y obtengan la autorización, por parte del Organismo Licenciante, para actuar como Autoridades Certificantes de sus propios agentes. Es decir que, cumplidos los recaudos exigidos por el Decreto mencionado, podrán emitir certificados de clave pública a favor de sus dependientes.

3.2.19 Procedimientos

1) Licenciamiento.

El licenciamiento es el procedimiento por el cual el Organismo Licenciante emite un certificado de clave pública a favor de un organismo público (quien adquiere la calidad de Autoridad Certificante Licenciada), quedando éste habilitado para emitir certificados a favor de sus dependientes.

Para obtener dicha licencia, el postulante debe completar un formulario de solicitud y adjuntar un requerimiento de certificado PKCS#10 en formato PEM.

2) Revocación.

La revocación es el procedimiento por el cual el Organismo Licenciante cancela la autorización otorgada a la Autoridad Certificante Licenciada para emitir certificados.

Esta cancelación puede efectuarse a solicitud de esta última o bien por decisión del Organismo Licenciante, según las pautas establecidas en la Política de Certificación.

Si una Autoridad Certificante Licenciada desea pedir al Organismo Licenciante la revocación de su certificado, puede utilizar un formulario de solicitud de revocación.

3.2.20 Laboratorio de Firma Digital

Para optimizar el proceso de difusión de la tecnología de Firma Digital, se ha implementado un Laboratorio, donde el público en general, y particularmente los funcionarios y agentes de la Administración Pública Nacional, experimen-

ten la generación de un par de claves, la gestión de su propio certificado y el envío de correo electrónico firmado, al tiempo de ofrecerse información diversa sobre esta tecnología.

Actualmente el Laboratorio cuenta con un nuevo circuito de certificados personales con validación a través de Autoridades de Registro.

3.2.21 Comprobación de la entidad del firmante

En primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

Tras bastidores, las firmas digitales dependen de un par de algoritmos matemáticos, denominados clave, que utilizan el remitente y el destinatario del mensaje. Estas claves se encargan de establecer la correspondencia que permite a la computadora del destinatario reconocer la computadora del remitente y certificar la autenticidad de un mensaje.

Una de las claves, la clave privada de la persona, está alojada en la PC o registrada en una tarjeta inteligente, e identifica que un mensaje ha sido enviado por la persona. La segunda es una clave pública, que puede ser empleada por cualquiera que desee autenticar documentos que la persona firme. La clave pública 'lee' la firma digital creada por la clave privada de la persona y verifica la autenticidad de los documentos creados con la misma.

La clave privada de la persona se desbloquea mediante una contraseña. En el futuro, para mayor seguridad aún, este sistema de clave y contraseña podría ser reemplazado por tecnologías biométricas, que miden características del cuerpo humano, como la retina, una huella digital o un rostro asociado con un registro de identidad.

3.2.22 Certificado Digital Propio

En nuestro país, la Infraestructura de Firma Digital del Sector Público Nacional pone a su disposición una Autoridad Certificante gratuita a través de la cual podrá obtener su propio certificado digital.



Figura 3.12: Autoridad Licenciante Certificada.

Utilizando este certificado usted podrá asegurar todas sus comunicaciones de correo electrónico, garantizando su autoría y la integridad del mensaje.

3.2.23 Obtención de una Firma Digital

Para enviar una firma digital, se requiere en primer lugar registrarse en una autoridad de certificados y solicitar el certificado de identidad digital, que hace de la firma un instrumento único. La mayoría de las autoridades de certificados también proporciona el software necesario y ofrece asesoría al usuario en el proceso de obtención, instalación y utilización de la firma digital.

La persona debe llenar un formulario de solicitud y suministrar pruebas de identidad para obtener el certificado. La firma digital se anexa a un mensaje de e-mail de manera muy similar al de los archivos.

3.2.24 Autoridad Certificante Licenciada

Subsecretaría de la Gestión Pública.

A la fecha, se han otorgado licencias a favor de las siguientes Autoridades Certificantes en el marco del Decreto 427/98:

- Autoridad Certificante Licenciada del Ministerio de Economía

Este es el certificado Raíz de la Infraestructura de Firma Digital del Sector Público Nacional.

- ArCert, Coordinación reemergencias en Redes Teleinformáticas.



Figura 3.13: Autoridad Licenciante.



Figura 3.14: Autoridad Licenciante.

Descripción: Autenticación del ingreso a bases de datos de la Coordinación de Emergencias en Redes Teleinformáticas para la Administración Pública Nacional.

Usuarios: Organismos Públicos.

Inicio de Operaciones: 08/1999.

- Ministerio de Economía.

Circuito Interno de Correo Electrónico firmado digitalmente.

Descripción: Circuito interno de comunicación de textos de resoluciones firmadas dentro del ministerio y áreas dependientes.

Cantidad de Usuarios: 150 aprox.

Inicio de Operaciones: 01/1998.

- Comisión Nacional de Valores.

Autopista de la Información Financiera (AIF).

Descripción: Proyecto desarrollado con el objetivo de recibir y publicar por Internet, a beneficio del público inversor nacional e internacional, la información financiera de las principales empresas del país que cotizan sus acciones



Figura 3.15: Energía Atómica.

y obligaciones negociables en el ámbito bursátil. Algunos ejemplos de información firmada digitalmente recibida por la AIF son: estados contables, prospectos informativos de emisión de acciones y de obligaciones negociables, estatutos, actas de asamblea, calificaciones de riesgo de títulos valores, notificaciones de eventos económicos significativos.

Usuarios: 120 Agentes CNV; 200 Empresas Cotizantes; 12 Calificadores de Riesgo; 200 Fondos Comunes de Inversión.

Inicio de Operaciones: 04/1999.

- Comisión Nacional de Energía Atómica.

Circuito Interno de Correo Electrónico firmado digitalmente.

Descripción: Circuito de comunicaciones a través de correo electrónico firmado dentro del organismo.

Cantidad de Usuarios: 50 aprox.

Inicio de Operaciones: 11/1998.

- Poderes Judiciales Provinciales.

Convenios de Comunicación Electrónica Interjurisdiccional y Sistema de Información para la Justicia Argentina.

Descripción: Los Convenios fueron firmados en la sede del Ministerio de Justicia y Derechos Humanos el 6 de Septiembre de 2001 por la casi totalidad de los Poderes Judiciales del país, la Procuración General de la Nación y la Defensoría General de la Nación. Promueven la utilización del correo electrónico firmado digitalmente en las comunicaciones entre organismos judiciales de

distinta jurisdicción territorial. El artículo 5° del Protocolo Técnico establece que, hasta tanto las Partes organicen su propia Autoridad Certificante, los certificados digitales serán emitidos por alguna de las partes o por la AC de la Subsecretaría de la Gestión Pública, y los firmantes se constituirán como Autoridades de Registración.

3.2.25 Certificados Digitales

Mediante la criptografía podemos establecer comunicaciones seguras con otras personas. ¿Pero esas personas son quienes dicen que son?. ¿Quién nos lo asegura?.

Para resolver este problema surgen unas entidades, que tienen que ser de confianza para todo el mundo. Estas entidades "certifican" las claves públicas de los usuarios que se las remiten emitiendo un certificado.

Existen cuatro tipos de certificados, cada uno de ellos ofrece un nivel de seguridad diferente.

Los certificados los tiene que conceder "alguien". Tiene que haber una tercera parte, de confianza para emisor y receptor, que certifique a ambos. Estas terceras partes reciben el nombre de "Trusted Third Parties (TTP)", terceras partes de confianza. Su labor, básicamente, consiste en identificar a usuarios, empresas o servicios con una determinada clave pública. Las entidades que emiten certificados reciben el nombre de "Certification Authority (CA)", las cuales han de ser de confianza y pueden estar certificadas por ellas mismas o por otra CA superior.

Básicamente un certificado esta compuesto por varios campos:

- Identidad del propietario.
- Clave pública.
- Periodo de validez.
- Identidad.
- Clave pública de la CA que lo expidió.
- Firma digital del certificado (realizada por la CA).

La seguridad de un certificado reside en la confidencialidad de la clave privada. Al ser los certificados de dominio público cualquiera puede comprobarlos

y lo único que le certifican es quien es el propietario de una determinada clave pública. Ese propietario es la “única” persona que conoce la clave privada correspondiente a la pública certificada.

La persona que conozca una determinada clave privada puede certificarse utilizando el certificado de la correspondiente clave pública y de esta forma ofrecer una “falsa” seguridad a la persona que ha verificado el certificado (suplantación de personalidad).

Cuando un certificado ha sido revocado la CA que lo expidió lo coloca en su certificación “Revocation Lists (CRL)”, lista de revocación de certificados. [5]

Cuando queremos establecer una comunicación con “alguien” debemos poseer su clave pública. Una vez conseguida debemos asegurarnos que es quien dice ser. Para ello solicitamos su certificado y comprobamos su validez de la siguiente forma:

- Comprobamos su caducidad.
- Comprobamos que CA lo expidió.
- Comprobamos el certificado de la CA, así como todos los certificados de CA's superiores que haya, si se da el caso, certificado a la CA anterior.
- Comprobamos que el certificado no fue manipulado, comprobando la firma digital de la CA.
- Comprobamos CRL de la CA para verificar que no ha sido revocado.
- Después de todo esto podemos establecer una conexión “segura” y “autenticada”.

Bibliografía

- [1] Jorge Ramió Aguirre. *Seguridad Informática y Criptografía*. Departamento de Publicaciones EUI, Universidad Politécnica de Madrid, España, 2003.
- [2] Jorge Sánchez Arriazu. *Descripción del Algoritmo DES*. España, 1999.
- [3] N.Ñaor; B.Pinkas. *Visual Authentication in Advances in Cryptology - CRYPTO 1997*. B. Kaliski, NJ-USA, 1997.
- [4] A. Fúster; F. Montoya; D. de la Guía Martínez; J. Muñoz. *Técnicas Criptográficas de Protección de Datos*. Editorial RA-MA, Madrid, España, 1997.
- [5] P. Caballero Gil. *Introducción a la Criptografía*. Editorial RA-MA, España, 1996.
- [6] P. Caballero Gil; C. Hernandez. *Criptografía y Seguridad de la Información*. Editorial RA-MA, España, 2001.
- [7] Manuel José Lucena López. *Criptografía y Seguridad en Computadores*. España, 2002.
- [8] N.Ñaor; A. Shamir. *Visual Cryptography, in Advances in Cryptology - Eurocrypt 1994*. A. De Santis, NJ-USA, 1995.

Índice de Materias

- Algoritmo de encriptación
 - aplicación, 5
- Algoritmo DES
 - comparación, 61
 - etapas, 54
 - múltiple, 57
 - origen, 54
 - seguridad, 55
 - variantes, 57
- Algoritmo El Gamal
 - definición, 62
- Algoritmo IDEA
 - definición, 57
 - seguridad, 57
- Algoritmo RSA
 - comparación, 61
 - origen, 59
 - protocolo, 59
 - robustez, 59
 - seguridad, 61
- Algoritmo DSA
 - definición, 63
- Ataques
 - consecuencias, 26
- Auntenticación
 - definición, 16
- Capacidades
 - definición, 34
- Cerificado Digital
 - componentes, 84
- Certificado Digital
 - definición, 84
 - Seguridad, 84
- Cifrado de César
 - concepto, 43
- Cifrado de Feistel
 - definición, 52
- Cifrado en Bloque
 - componentes, 52
- Clave Asimétrica
 - definición, 6
- Clave Pública
 - definición, 58
- Clave Privada
 - definición, 58
- Clave Simétrica
 - definición, 5
 - riesgo, 6
- Claves
 - mecanismo, 35
 - tipo, 5
- claves Diffie-Hellman
 - acuerdo, 47
- Comercio Electrónico
 - en qué consiste?, 3
 - entorno jurídico, 4
 - seguridad, 19
- Confidencialidad
 - definición, 15
- Control
 - definición, 16
- Crfrado de Flujo

- definición, 51
- Criptografía
 - controversia, 45
 - Mecanismo básico, 5
 - origen, 5
 - principal objetivo, 5
 - ramas, 45
- Criptografía Asimétrica
 - desventaja, 7
 - origen, 58
 - ventaja, 6
- Criptografía Simétrica
 - clasificación, 49
 - desventaja, 49
- CRP4, 49
- Dato
 - definición, 17
- Delito Informático
 - definición, 28
- Desencriptación
 - definición, 5
- Disponibilidad
 - definición, 16
- Dominios de Protección
 - definición, 32
- Easy sign
 - software, 77
- Encriptación
 - definición, 5
- Estrategias de Seguridad
 - pasos generales, 29
- Estructura de Grupo
 - definición, 45
- Firewall
 - definición, 39
- Firma Digital
 - aplicaciones, 73
 - concepto, 6
- funcionamiento, 71
- infraestructura, 77
- métodos, 6
- seguridad, 73
- ventajas, 7, 69
- Función Hash
 - definición, 7
- Identificación Física
 - definición, 36
- Información
 - definición, 17
- Integridad
 - definición, 16
- Intrusos
 - herramientas, 25
- Listas de Acceso
 - definición, 34
- Matriz de acceso
 - definición, 33
- Mecanismos de Autenticación
 - definición, 35
- Mecanismos de autorización
 - definición, 32
- Monoalfabéticos
 - definición, 44
- Penetration Test
 - componentes, 37
 - objetivo, 37
- Penetration Testing
 - definición, 25
- PGP
 - definición, 9
 - ejemplo, 12
 - estructura operativa, 10
 - ventajas, 9
 - versiones, 10
- PKI

- definición, 8
- objetivos, 8
- Política de Seguridad
 - definición, 30
- Polialfabéticos
 - definición, 44
- Protocolo SSL
 - uso, 6
- Routers
 - definición, 41
- Seguridad
 - aspecto importante, 2
 - problema, 2
 - problemas, 18
- Seguridad Física
 - amenazas, 23
 - definición, 21
- Seguridad Informática
 - definición, 15
 - propiedades, 15
- Seguridad Lógica
 - definición, 23
 - objetivos, 24
- Sistemas Criptográficos
 - clasificación, 44
- Sistemas de detección de intrusos
 - definición, 36
- Texto Plano
 - definición, 43
- Trampas de Red
 - definición, 38
- Trusted Third Parties
 - funcion, 84