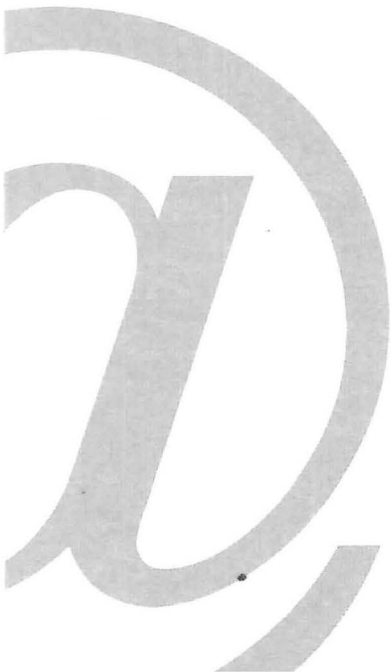

La seguridad en la Red

José Luis González Sánchez

La seguridad en la Red

1 Introducción

El importante empuje que *Internet* está imprimiendo a las comunicaciones por medios electrónicos ha quedado ya patente. Aunque la primera preocupación fue hacer posible esa comunicación, no ha tardado en aparecer otro aspecto importante en el mundo de las comunicaciones humanas como es la **seguridad de la información** transmitida.

Inicialmente la seguridad quedó, en cierto modo, descuidada. Pero a medida que la *Red* va popularizándose, y cuando se han sufrido ya importantes ataques a la seguridad de la información, va surgiendo una gran concienciación por este relevante aspecto para un **canal de comunicación y de transmisión de información** como es *Internet*.

Existen ciertos factores que considerar y reforzar para conseguir la ya obligatoria seguridad para muchos usuarios de ***Internet*** e ***intranets***. Los **Sistemas Operativos** no son todo lo seguro que cabría esperar; lo mismo podría decirse de los **protocolos y tecnologías** sobre las que descansan las comunicaciones; pero, posiblemente, la mayor debilidad, en lo que a seguridad se refiere, está en la **excesiva confianza**, **desconocimiento**, o posible **negligencia** de los **usuarios** y **administradores** de los sistemas informáticos y las comunicaciones.

Se impone, por tanto, conocer dónde se encuentran las **debilidades** más importantes para poder conjurarlas estando, en la medida de lo posible, por delante de los amigos de la información ajena. Con este objetivo se presenta el siguiente artículo y, primordialmente, con la intención de tranquilizar a todos aquellos usuarios sensibilizados con la **privacidad** de su información y la **intimidad** de su comunicación a través de un canal tan importante como es *Internet*. Éste es un trabajo dirigido, en mayor medida, a los administradores de sistemas multiusuario y responsables de comunicaciones, pero consideramos que la seguridad es un aspecto de vital importancia por lo que ningún *cibernauta* debería permanecer ajeno a los conceptos y problemáticas que van a ser presentados.

Los usuarios de *Internet* sensibilizados con los problemas relacionados con la inseguridad pueden encontrar en las soluciones propuestas en este artículo la necesaria tranquilidad que les anime a usar sin preocupaciones servicios tan importantes como la mensajería electrónica y la telecompra.

2 Seguridad de la información

La *seguridad informática* es la encargada de proteger el ordenador y todo lo relacionado con él (acceso al edificio, cableados y equipos periféricos) a esto suele llamársele, también, *seguridad de la información.*

Más concretamente, suele hablarse de seguridad informática relacionándola con accesos a sistemas informáticos por personas no autorizadas con la intención de: obtener información valiosa; demostrar que han conseguido entrar; destruir información; venganza o espionaje contra la organización atacada; etc. .

Pero existen otros peligros para la información menos espectaculares pero más habituales como son los errores humanos; inexistencia de copias de seguridad; compartir contraseñas (*passwords*); en suma, inexistencia de lo que se conoce como política de seguridad.

Los tres pilares básicos de la *seguridad informática* son:

- *Confidencialidad*: La información no debe ser visible para ojos no autorizados.
- *Integridad*: La información no debe ser modificada por personas no autorizadas.
- *Disponibilidad*: La información debe estar siempre al acceso de sus propietarios.

Pero la base sobre la que descansa toda seguridad es la correcta configuración de los sistemas y las comunicaciones y, sobre todo, el seguimiento día a día, ya sea como responsables de los sistemas o como usuarios finales de los mismos, que permita detectar, en todo momento, cualquier amenaza o incidente relacionado con la inseguridad de la información.

3 Política de seguridad

La política de seguridad puede ser entendida como un conjunto de reglas que implementan una serie de mecanismos y servicios necesarios para garantizar un nivel de seguridad adecuado sobre los recursos informáticos disponibles en una organización.

La política de seguridad debe proteger los tres puntos generales siguientes:

1.- La información contenida en los sistemas informáticos que siempre tiene valor:

-Cuando se revela se pierde la *Confidencialidad.*
-Cuando se altera se incumple la *Integridad.*
-Cuando no está accesible no se garantiza la *Disponibilidad.*

2.- Los recursos de los sistemas informáticos:
-Accesos no autorizados y abusivos para diversos fines.
-Destrucción de los mismos.
-Monopolización de recursos valiosos (CPU, discos, memorias)
-Sabotaje de parte, o todos, los recursos.

3.- La reputación:
-Propia de cada usuario.
-Del grupo de trabajo, departamento o unidad funcional.
-De la organización completa.

La política de seguridad de la organización debe concretar además:
- Por qué se establece la protección.
- Cuál es el verdadero valor y coste de la misma.
- Quién asume la responsabilidad y de qué autoridad dispone el responsable.

Características de la política de seguridad:
- Debe ser sencilla, precisa y fácil de entender por toda la organización.
- Toda la organización debe conocerla y entenderla por lo que debe participar en su diseño.
- El responsable de la misma debe disponer también de autoridad para aplicarla.
- La política establecida debe proteger la propiedad, reputación y actividad de la organización.
- Debe cuidar tanto a la información como a los recursos humanos.
- Las amenazas y conflictos se resolverán atendiendo a la política establecida.

La mayor parte de las redes actuales y, sobre todo *Internet*, se pensaron para usuarios dignos de confianza. Como cabía esperar, este planteamiento se ha constatado ya como demasiado optimista y no han tardado en aparecer usuarios de la *Red* que no han dudado en pervertirla.

Con la popularización de las tecnologías de redes han empezado a producirse ataques a la información que viaja por ellas tipificándose en dos grandes grupos:

- *Ataques activos*: Manipulación de los datos, tergiversando la información.
- *Ataques pasivos*: *"Escucha"* del tráfico que atraviesa la red sin actuar sobre él.

Tradicionalmente se ha distinguido también entre *seguridad perimétrica* o *exterior* y *seguridad interna,* y entre *seguridad física* y *seguridad lógica.* Sin embargo no vamos a detenernos en estos aspectos más generales, aunque es importante llamar la atención del lector para destacar que la mayor parte del artículo se centra en la *Seguridad Lógica* que está relacionada con el software que se utiliza para velar por la seguridad de las comunicaciones a través de la *Red.*

4 Debilidades de los sistemas informáticos

Seguidamente se exponen los tres puntos de debilidad más importantes en los sistemas informáticos que son los, habitualmente, utilizados por aquellos usuarios sin escrúpulos que no dudan en sacar ventaja de ellos cuando los detectan en un sistema que les interesa por una causa u otra.

4.1 SISTEMAS OPERATIVOS DÉBILES

El acceso no autorizado a los sistemas multiusuario habitualmente utilizados como *servidores en Internet*, o como ordenadores centrales en grandes o medianas organizaciones, se produce por *agujeros* de seguridad en los propios sistemas que, como poco, deberían estar a *nivel C2* de seguridad.

Los ordenadores personales, por su arquitectura o por los sistemas operativos que soportan, no permiten implementar avanzados mecanismos de seguridad. Pero en el caso de *Internet* esto no es importante pues, a parte de no ser posible acceder a ordenadores personales (con Sistema Operativo monousuario) conectados a ella, lo que más interesa a los *piratas informáticos* son los potentes *servidores* accesibles a través de la *Red*. Lo que sí es cierto, es que la mayor parte de ataques a la información suele realizarse desde ordenadores personales.

Los sistemas multiusuario como *Unix*, ampliamente utilizado para soportar *servidores* en *Internet*, padecen peligrosos *agujeros* de seguridad que es como se conocen en la jerga las debilidades o vías de acceso a la información privada. Entre esos agujeros pueden destacarse:

- El programa *sendmail* en versiones bajas. Se solventa con parches o con instalación de versiones superiores. A pesar de los parches, periódicamente siguen apareciendo nuevas debilidades del sistema de mensajería electrónica propio de *Unix*, que implica la actualización de nuevas versiones.

- Fichero */etc/passwd* que es legible para cualquier usuario que accede al sistema. Puede evitarse usando el mecanismo de *shadowing* o *security password*.

- Servicio *finger* usado desde cualquier nodo en la red para averiguar los usuarios que están conectados a cada nodo en todo momento y probar a averiguar su *password* o contraseña.

Los citados son algunos ejemplos de *agujeros* de seguridad conocidos en *Unix*, pero no son los únicos; del mismo modo que *Unix* tampoco es el único sistema multiusuario con debilidades, piénsese también en *Windows NT* y otros.

Seguidamente se destacan los que podrían considerarse como aspectos más importantes de un Sistema Operativo seguro:

Integridad de la información, que evita la alteración de la información por usuarios no autorizados.

Disponibilidad de todos los recursos del sistema (CPU, memoria, discos, periferia).

Intimidad de la información contenida para todos los usuarios.

Consistencia que garantiza los cambios en el modo de funcionamiento del sistema.

Aislamiento que impida el acceso de intrusos al sistema que pongan en peligro alguno, o todos los puntos anteriormente expuestos.

Para los interesados en los diferentes niveles de seguridad de los sistemas operativos, destacar que existe el *Documento DoD 5200.28-STD* de Diciembre de 1985, conocido como el *Orange Book (Libro Naranja)* que establece los diferentes niveles o requerimientos de seguridad que éstos deben cumplir. De la lectura de *El Libro Naranja* puede concluirse que, en la actualidad, no debería admitirse un nivel de seguridad inferior al *C2* en ningún sistema multiusuario conectado a *Internet*, vaya a usarse éste como *servidor* de cualquiera de los servicios de *Internet* conocidos o, solamente, para soportar las cuentas de usuario que actuarán como *clientes* de otros *servidores*.

Lo comentado no sólo interesa a los responsables de sistemas, sino también a todos los usuarios de *Internet* que tengan *cuentas* en sistemas multiusuario inseguros. Sepa que si es así, su información puede quedar al acceso de infinidad de aprovechados, espías o, generalmente, usuarios con espíritu de portera *chinchorrera*.

4.2 COMUNICACIONES INSEGURAS

Las protocolos de *Internet* se diseñaron deliberadamente para que fuesen simples y sencillos de forma que, tanto las *Aplicaciones* como el *Nivel de Transporte*, carecen de mecanismos de seguridad, lo que ha desempeñado un papel importantísimo para su implantación. Cada mes hay cientos de avisos desde todas las partes del mundo denunciando *IP spoofing* intentando burlar el protocolo *IP*.

Las redes de área local como *Ethernet* tampoco tienen implementados mecanismos de seguridad lo que posibilita la existencia de *sniffers* que pueden *"escuchar"* los paquetes que viajan por la red. Cada día aparecen nuevos avisos de este tipo de ataques instalados en nodos comprometidos como ordenadores personales no controlados, o en grandes sistemas descuidados en cuanto a la seguridad se refiere.

Además, son habituales los ataques a *NFS (Network File System o sistemas de ficheros accesibles por red)* que acaban ganando acceso a cuentas privilegiadas de *root* usadas por los administradores del sistema.

4.3 USUARIOS CONFIADOS

Los administradores de sistemas por dejadez, desconocimiento y, generalmente, por falta de tiempo, no cuidan los posibles *agujeros de seguridad* existentes en los sistemas y en las comunicaciones. En algunas organizaciones, los administradores del sistema son los responsables de establecer la política de seguridad de la organización, y de educar a los usuarios de sus sistemas para que se conciencien de los problemas que implica la inseguridad. Lo ideal sería la existencia de la figura del responsable de seguridad encargado de implementar la política de seguridad.

Los usuarios de los sistemas, también por dejadez o desconocimiento no ponen los medios adecuados para evitar que su información quede al acceso de usuarios no autorizados.

Como ya es sabido, las cuentas en los sistemas multiusuario están protegidas de accesos indebidos con el uso de *passwords* o contraseñas debidamente encriptadas que sólo debería conocer el propietario de cada cuenta de usuario para garantizar la privacidad de su información. Cada usuario es responsable de controlar sus *passwords* y esto es, en sí mismo, un problema, ya que no todas las contraseñas son adecuadas como se va a demostrar.

Con medios informáticos, en 5 ó 10 minutos puede encriptarse y compararse un diccionario de 250.000 palabras. Si se usa una contraseña lo suficientemente sencilla como para estar entre esas 250.000 palabras, en poco tiempo puede ser descubierta.

Si es usted usuario de algún sistema multiusuario conectado, o no, a *Internet* la siguiente estadística le interesa.

Daniel V. Klein realizó un estudio con 13.797 cuentas de usuarios de todos los EUA para intentar averiguar el mayor número de contraseñas posible y obtuvo estos alarmantes resultados usando un diccionario de poco más de 85.000 palabras habituales compuesto según se indica en la ***Tabla 1***.

Las datos indican que, con un sencillo diccionario, pudieron descubrirse casi la cuarta parte de las contraseñas intentadas, lo que debería hacer reflexionar a cualquiera antes de elegir una *password* de acceso a su cuenta de usuario en un sistema que forme parte de *Internet*.

Para evitar situaciones como la descrita se sugieren las siguientes recomendaciones para elegir una buena contraseña:

- Mezclar mayúsculas, minúsculas y caracteres no alfabéticos.
- Longitud mínima de 6 caracteres.
- No usar palabras de diccionarios, ni con sentido, ni nombres propios.
- Debe contener números, pero no sólo números.
- No compartirla con nadie ni escribirla en ningún sitio y ser fácil de recordar.
- No debe ser números de teléfono, ni DNIs, ni matrículas de vehículo ni ningún dato personal que pueda ser relacionado con su propietario de forma evidente.

- Cambiarla, como poco, una vez al mes.
- No usar la misma en ordenadores diferentes.

Grupos de palabras	Tamaño del diccionario	% aciertos
Secuencias de caracteres	866	0,2
Números	450	0,1
Palabras chinas	398	0,4
Lugares	665	0,6
Nombres comunes	2.268	4,0
Nombres de hombres	4.955	1,2
Nombres de mujeres	3.091	1,0
Nombres poco comunes	5.559	0,9
Mitos y leyendas	1.357	0,5
Personajes de Shakespeare	650	0,1
Términos deportivos	247	0,2
Ciencia ficción	772	0,4
Películas y actores	118	0,1
Dibujos animados	133	0,1
Personajes famosos	509	0,4
Frases hechas	998	1,8
Apellidos	160	0,1
Términos biológicos	59	0,0
Contenidos en /usr/dics/words	24.474	7,4
Nombres de hosts	12.983	1,0
Mnemotécnicos	14	0,0
Términos de la Biblia	13.062	0,6
Palabras diversas	8.146	0,4
Asteriodes	3.459	0,1
TOTALES	85.393	21,6 %

Tabla 1 *Contraseñas más utilizadas*

5 *Hackers y crackers*: el mito de *Dr. Jekill y Mr. Hyde*

Para comprender adecuadamente a qué nos enfrentamos es necesario conocer algunos conceptos y, sobre todo, la personalidad de esos usuarios aventajados que no dudan en aprovechar las flaquezas comentadas anteriormente.

Hacker: Usuarios que tienen altos conocimientos informáticos y que son capaces de ejercerlos con finura. Una de las más acertadas definiciones de este tipo de usuarios informáticos es quizás la dada por Cristopher Stoll en su libro «*El Huevo del Cuco*». *"Los que así se autodenominan, o gustan que les denominen, son genios del software, capaces de salir de situaciones difíciles con su programación creativa. Conocen todos los recovecos del sistema, son programadores creativos incapaces de abandonar el ordenador hasta que la máquina esté satisfecha. Se identifican con el ordenador como si de un amigo se tratase."*

Ellos se autodenominan como idealistas altruistas y románticos cuya aspiración es lograr que la información circule libremente por *Internet*. Cuando consigue algo de interés, el *hacker* lo compartirá con los demás componentes de su círculo.

Los orígenes de la palabra *hacker* podrían estar en la forma en que los empleados de telefónica solían reparar algunos problemas técnicos, de un golpe fuerte y seco (*hack*). Los que practicaban el *hack* acabaron siendo *hackers*, y la técnica se extendió también a los antiguos ordenadores de válvulas que solían salir de más

de un problema con una buena palmada en el costado. Esto acabó de extender el término al mundo de la informática que identifica como *hacker* a todo aquel que practica la intrusión sigilosa y sin autorización en un sistema informático.

Cracker: estado ambiguo en que se encuentran algunas personas empeñadas en acceder a los sistemas o información de otras personas. Suele llamárseles también *crashers* por su comportamiento destructivo en los sistemas que consiguen violar. Exponen razones débiles para hacerlo, entre ellas dicen que lo hacen porque es posible, pero más probablemente lo hacen por el morbo de hacer algo ilegal o ilícito o, también, para ganar prestigio dentro de su grupo o círculo.

Ciertos grupos de *crackers* antisociales realizan actos vandálicos borrando discos, provocando *crashes* de sistemas, matando procesos, suplantando personalidades, tergiversando informaciones, etc..

A algunos de estos grupos se les considera auténticos terroristas o salteadores de las redes. Estos burladores de la ley se han apoderado del término *hacker* y están creando bastante confusión. Además del término *cracker* ya empieza a usarse el de *petardo, ciberpunk o computervredebreuk* (literalmente, transtornador de la paz del ordenador en holandés).

Phreakers: Así se autodenominan inicialmente aquellos que conseguían utilizar las líneas telefónicas sin pagar o pagando tarifas lo más reducidas posible. Por asimilación, este término se asocia también a aquellos usuarios de *Internet* que consiguen acceder a servicios de pago sin pasar por taquilla.

En cualquiera de sus acepciones, este tipo de usuario informático suele tener un perfil psicológico y social bastante definido:

- Suelen ser jóvenes, generalmente estudiantes avispados o profesionales de la informática, y con elevados conocimientos por tanto.
- Personas solitarias y con bastante tiempo libre y egocéntricos en ciertos casos.
- Se reafirman en su personalidad con este tipo de vandalismos anónimos.
- Su mayor satisfacción la alcanzan burlando cualquier sistema de seguridad y dejando las marcas de su entrada para poder autoafirmarse ante su grupo pudiendo demostrar sus fechorías.
- En ocasiones, utilizan sus conocimientos con afán vengativo ante determinadas situaciones que les perjudican.
- Huyen de las tareas rutinarias de la vida cotidiana y les atrae el riesgo de lo prohibido y la estimulación mental que provoca saltarse las reglas.
- Son ordenados, metódicos y abiertos intelectualmente, pero caóticos en el resto de sus actividades.
- Suelen mantener reuniones y congresos donde intercambiar sus experiencias, e incluso disponen de foros de discusión en las *news* como *alt.hackers*, *alt.2600* ó *alt.ciberpunk*.

Puede decirse en su descargo que *hackers* y *crackers* han colaborado a que afloren gran parte de las debilidades aquí expuestas pero, en muchas ocasiones, sus fechorías no han sido tomadas tan en serio como debería, bien sea por la falta de jurisprudencia, o por un punto de vista demasiado romántico de esas actividades que ha impedido calibrar debidamente los daños causados.

En cualquiera de sus acepciones, este tipo de usuarios de la *Red,* envueltos en ese halo misterioso y romántico que les confiere el ser considerados como quijotescos genios de la informática puede estar realizando bastante daño al resto de usuarios desde el momento que infringen una norma que cualquier Gobierno considera como básica y que es el derecho a la intimidad.

6 Descripción de ataques reales a través de *Internet*

La historia de *Internet* está llena de ataques sufridos desde dentro de ella misma. Queremos destacar algunos de los más importantes y peligrosos incidentes con la intención de que su conocimiento impida que la historia se repita.

6.1 THE *WORM* (*EL GUSANO DE INTERNET*)

El caso más conocido de ataque a una red informática fue el sufrido por *Internet* el Miércoles 2 de Noviembre de 1988 por el denominado *gusano de Internet.* Se originó en la *Universidad de Cornell* y se extendió rápidamente a las de *Stanford, California, Princeton,* al *MIT* e incluso a la *NASA.* Afectó a un total de 6.000 ordenadores y provocó unas pérdidas cuantificadas en 10.000 millones de Ptas..

Su autor Robert T. Morris expuso que realizaba unas prácticas para sus estudios con algún *"bug"* (fallo de programación) lo que provocó que *"el gusano se le fuese de las manos".* Destacar que el autor de *Worm* es el hijo del entonces director de la *Agencia de Seguridad Nacional (NSA)* americana.

Worm recopilaba información sobre usuarios, nodos y redes que usaba para luego conectarse a ellos. Aprovechó las debilidades del sistema operativo *Unix (Sun3 y Ultrix), finger, sendmail y /etc/passwd.* También aprovechó los sencillos mecanismos de red (protocolo *IP*) implementados para mejorar la conectividad de *Internet* que, como ya es sabido, se pensó con una filosofía abierta para facilitar la comunicación.

Síntomas de la infección:

- Aparición de ficheros desconocidos en el directorio */usr/tmp.*
- Colapso de los nodos que eran incapaces de continuar *"vivos".*

Worm se dividía en dos partes:

- *Programa de arranque* usado para infectar. Cuando éste conseguía acceder a un ordenador se traía hasta él el *programa principal o virus* y el *programa de arranque* continuaba con otro nodo.

- *Programa principal* o *investigador*: Recopilaba información sobre nodos de la red a los que conectarse mediante utilidades de los propios sistemas. Elegida la víctima intentaba el contagio a través de los comentados agujeros de seguridad de *Unix*. En líneas generales, el programa principal realizaba la tarea de averiguar a qué otros nodos de la red se podía autocontagiar siguiendo los siguientes pasos:

Uno de cada siete gusanos se hacía inmortal, y realizaba un *fork* (creando procesos hijo) de manera periódica *"matando"* a su proceso padre con los siguientes objetivos:

- El *fork* cambiaba el identificador de proceso lo que complicaba su detección.
- No se acumulaban excesivos consumos de tiempos de CPU que alertasen a los *systems managers*.
- Conseguía restaurar la prioridad normal de procesos que se pierde cuando un proceso lleva mucho tiempo ejecutándose.

Cada 12 horas se borraban los nodos ya infectados y los inmunes de la tabla elaborada, lo que provocaba que las máquinas pudiesen volver a infectarse o tuviesen varios gusanos a la vez.

6.2 EL *HACKER* DE HANNOVER

En el *Lawrence Berkeley Laboratory* un error de 75 centavos en el *accounting* (contabilidad) del sistema permitió a Cliff Stoll, administrador de los sistemas del LBL, descubrir el acceso no autorizado a sus sistemas de un *hacker* que, durante más de un año, usando las redes, accedió a varios ordenadores militares y centros de investigación americanos. Utilizó diversas técnicas y detrás de todo se encontraba una red de espionaje en Alemania Federal que vendía los ficheros a la *KGB* por dinero y drogas. La red fue desmantelada en 1.989.

Este ataque real ha sido magistralmente narrado en clave de novela de espionaje por el propio Stoll en su libro «*El Huevo del Cuco*». Este libro es una importante referencia para todos los concienciados con los incidentes de inseguridad de la información a través de las redes. Se recuerda que el cuco se caracteriza por poner sus huevos en el nido de otras aves con la egoísta esperanza de que éstas saquen adelante sus polluelos.

6.3 OTROS INCIDENTES RELACIONADOS CON LA INSEGURIDAD

Multitud de organismos públicos y universidades han sufrido también en sus instalaciones los efectos de las actividades de los *crackers* y *hackers*.

El 15 de Enero de 1.990 se produjo el llamado *crack telefónico de AT&T*. El conmutador de llamadas de larga distancia de esta compañía telefónica dejó de funcionar sin causa explicable quedando sin servicio telefónico a más de la mitad

de los Estados Unidos. Dos semanas fue el tiempo necesario para restablecer todo el servicio y la versión oficial del fallo dada por *AT&T* fue la existencia de un *bug* en el software que se había instalado recientemente en algunas estaciones telefónicas que se había extendido a varias de las centralitas del país.

Pero en el transfondo de todo el *crack telefónico* se hablaba de actividades de *hacking*, que, unido al elevadísimo coste en que se estimaron intencionadamente las pérdidas (1 billón de dólares), posiblemente provocó la puesta en marcha en 1.990 de lo que se llamó la *Operación Sun Devil* o *"la caza de hackers"* en una investigación de dos años en la que participaron más de 100 agentes federales, varios representantes de la ley y el orden y apoyada por los recursos de varias compañías americanas.

Otro incidente afectó al ordenador central de la *Comandancia para la Defensa de Norteamérica* en *Colorado Springs* que fue atacado por Kevin Mitnik que destruyó y alteró datos en los ficheros que mantenían información de su propia libertad condicional en la que se encontraba por dedicarse a alterar y desconectar las conversaciones telefónicas de diversas personalidades. La compañía informática *DEC (Digital Equipment Corporation)* valoró económicamente el daño producido en más de cuatro millones de dólares.

Se ha podido comprobar que algún estudiante despechado contra su propia universidad ha usado *Internet* para ejercer un dudoso derecho al pataleo destrozando trabajos de investigación, prácticas de sus compañeros y haciendo perder múltiples horas de trabajo a los responsables de los equipos informáticos dañados. Tras las investigaciones pudo saberse que, una vez averiguada (*crakeada*), la contraseña de *root* del sistema *Unix* violado el estudiante saltó desde España a América desde donde volvió a su universidad para realizar las fechorías en un intento de actuar bajo el anonimato que *Internet* le permitía.

Estos han sido ejemplos de otros tantos ataques donde ni siquiera la *Casa Blanca* o el propio *servidor de Web de La Moncloa* en nuestro país han podido librarse de los caprichos de aquellos que argumentan que la responsabilidad no debería recaer en ellos, sino en los que permiten o no impiden el acceso.

7 Virus informáticos

Actualmente, éste es el problema de inseguridad informática de, nunca mejor dicho, mayor *"virulencia"*. Aunque la curva de creación de virus ya no es exponencial y no se dobla su número cada 9 ó 10 meses, aún se producen miles de virus anualmente.

A continuación se presenta la división general clásica de virus existentes:

- *Caballos de Troya*: Son los más habituales. Se esconden dentro de otros programas esperando a activarse en el momento más oportuno. Éstos son los

más peligrosos para los usuarios de *Internet*, ya que puede ocurrir que usted esté *bajando* por la *Red* un software que le interese para instalarlo en su ordenador personal y no sepa que, en realidad, bajo esa apariencia se esconda cualquier maléfica intención.

La vía de contagio de virus clásica era la copia indiscriminada de software, pero en los últimos tiempos se están extendiendo importantes virus de la variedad de los *caballos de Troya* a través del correo electrónico. Los sistemas de mensajería como *Eudora* y *Pegasus* permiten el uso de *attachments* añadiendo a los mensajes ficheros con extensión *.DOC* que salen infestados del emisor y acaban transmitiendo el virus cuando llegan al destinatario.

Es necesario, por tanto, desinfectar con antivirus no sólo los ficheros que se introducen a través de disquetes, sino también los que lleguen a través de la *Red* sea por el servicio que sea (*news, E-mail, FTP*, etc.).

- *Gusanos*: Su hábitat suelen ser las redes y se propagan a través de ellas residiendo en la memoria de alguna de las máquinas que forman parte de la red. No suelen afectar a los discos, y lo mejor es reinicializar la red cuando se detectan.
- *Bombas lógicas o de tiempo*: Se activan cuando se dan ciertas circunstancias como fechas concretas o número de ejecuciones de un programa. Las bombas lógicas suelen ser la indeseable e inesperada manifestación de los *caballos de Troya*.

Son ejemplos de sistemas operativos infectables *MS-DOS, Macintosh, OS/2, Windows* y *Unix*. Existen también virus conocidos en LANs como *Netware*.

La solución a este importante problema quizás esté en la adecuada formación de los usuarios y en una apropiada legislación que controle la creación de este maléfico software que tanto daño está haciendo.

Como conclusión, tenga en cuenta que si usted es usuario de las *infopistas* desde ordenadores personales, deberá chequear cualquier software que obtenga a través de la *Red* antes de instalarlo en su ordenador. Piense que *Internet* se está convirtiendo en la más importante vía de contagio, por lo que hay que extremar las precauciones. Además, el correo electrónico se ha convertido en el hábitat preferido para los virus informáticos, aprovechando en muchos casos la ingenuidad de muchos usuarios que se aventuran a leer mensajes de remitentes desconocidos. Es destacable el hecho de que los virus no son responsabilidad de Internet, sino precisamente de los fabricantes de sistemas operativos que dejan ciertas debilidades sin resolver.

8 Leyes permisivas

La mayor parte de los problemas e incidentes relacionados con la inseguridad citados se producen porque no existe una legislación internacional que tipifique claramente los delitos informáticos. La mayoría de países tienen unas leyes demasiado permisivas en este sentido lo que da lugar a grandes vacíos legales. Por

ejemplo, en EUA no se lucha contra los creadores de virus porque esa actividad es considerada una forma de libertad de expresión.

En España contamos con la *LORTAD (Ley Orgánica de Tratamiento Automatizado de Datos de carácter personal)* que protege el derecho a la intimidad. Además, el *Código Penal* sanciona ya las conductas criminales cometidas usando como medio las tecnologías de la información o contra las tecnologías de la información del perjudicado. La mayor parte de expertos en aspectos legales coinciden en destacar que nuestro país cuenta con una de las legislaciones más avanzadas en estos aspectos.

Pero el mayor problema es la falta de esfuerzo común entre todos los países para luchar contra los ataques que provienen a través de las redes internacionales que siempre quedan impunes. Téngase en cuenta que *Internet* también convierte en virtuales las fronteras y esto afecta a las medidas legales que pueden ser aplicadas cuando los ataques se producen desde diferentes países sin la legislación adecuada. Por otro lado está la dificultad de obtención de pruebas y la demostración fidedigna del verdadero autor de los ataques a la seguridad informática.

Otro importante factor a tener en cuenta es la lenta evolución de las leyes respecto al dinamismo de los avances tecnológicos.

9 Técnicas para la violación de la información

Se exponen seguidamente los métodos usados por los *crackers* y *hackers* para aprovechar las debilidades que padecen los sistemas informáticos formen, o no, parte de *Internet.*

9.1 SNIFFERS

Desafortunadamente, son muy populares en la actualidad. Ya en 1.994 constituyeron el 80% de los ataques en todo el mundo. Son programas usados por los *crackers* para *"escuchar"* los paquetes que viajan por las redes (*Ethernet, DECnet*) filtrando el *username* y la contraseña en conexiones *telnet, rlogin, ftp,* etc. .

Se usan para visualizar o desviar información privilegiada. El uso más habitual es averiguar *passwords* de cuentas para, posteriormente, acceder a ellas.

Suelen usarse desde dentro de las propias organización que disponen de *LAN* y como un medio de acceder a información privilegiada. Las dos formas principales de detectarlos o evitarlos son las siguientes:

- El administrador de la red debe controlar toda máquina conectada a la red.
- El administrador de sistemas debe auditar su sistema para detectar fisgones que se manifiestan con procesos escuchando en los puertos *UDP 891* y *937* y *TCP 3011.*

Etherwatch:

Es un programa *sniffer Ethernet* que permite monitorizar la actividad de la red y puede ser usado para la identificación y diagnosis de problemas de red.

Permite monitorizar el tráfico basado en direcciones *Ethernet* (fuente, destino o ambas), tipo de protocolo (formato *Ethernet*), identificador de protocolo (*IEEE 802 Extended Format*) o combinación de todos esos modos.

Son necesarios privilegios para ejecutarlo en sistemas multiusuario, pero también es posible su instalación en ordenadores personales que, estratégicamente conectados a la red, pueden conseguir información valiosa de los usuarios conectados a esa red.

9.2 CRACKERS

Este es un software de dominio público pensado para ayudar a los administradores de sistemas multiusuario, que coincide en el nombre con los usuarios deshonestos que ya se han citado.

Trabaja sobre los ficheros de *passwords* (*/etc/passwd, SYSUAF.DAT,* etc) de sistemas multiusuario para averiguar qué usuarios han elegido contraseñas débiles al proteger sus cuentas.

Puede ser una herramienta muy peligrosa en las manos de *hackers* y *crackers*. En sistemas *Unix* sin *security password* es una puerta de entrada abierta a los piratas de la *Red*.

Debe localizarse su existencia en los sistemas, y la mejor manera de luchar contra esto es seguir la política de elección de *passwords* comentada anteriormente.

9.3 XWATCHWIN

Software de dominio público pensado con fines docentes. Permite capturar sesiones *Xwindow* de un nodo concreto y observar lo que realiza. Puede ser usado por los administradores de sistemas para auditar a presuntos *crackers* o *hackers*.

En manos de usuarios malintencionados puede ser también una herramienta muy dañina pues permite violar la intimidad de la persona observada sin que lo note.

Sólo permite capturar ventanas de *Xterminals* y de Estaciones de trabajo gráficas conectadas a la red en la que está la máquina que ejecuta el *Xwatch*. Sólo necesita conocerse el nombre del *host* que va a observarse.

La mejor forma de luchar contra *Xwatch* es detectar su existencia en el sistema y configurar *Xwindow* para no aceptar fisgones.

Existen otras herramientas similares para observar terminales *ascii* como *Supervisor* para *OpenVMS*.

9.4 HIJACKING (PIRATEO, SECUESTRO)

Esta técnica consiste en tomar el control de una conexión ya establecida de forma que trabaja el *hijacker* suplantando al usuario que realmente establece la conexión, el cual queda "colgado" y acaba retirándose o intentando una nueva conexión dejando al *hijacker* trabajando en el sistema bajo el más absoluto anonimato.

9.5 SPOOFING (BURLAR, HACERSE PASAR POR...)

Esta técnica puede aplicarse de diferente forma y, según el aspecto de *Internet* que intente burlarse, pueden distinguirse los siguientes tipos de *spoofing*:

- *IP spoofing*. Intento de "robo" de direcciones *IP*:
  Con el comando *nlsloop* puede observarse qué máquinas forman parte de una red.
  El comando *ping* puede usarse para comprobar cuáles de las máquinas anteriores están "vivas" y cuáles están paradas sea por la causa que sea.
  Se escoge una máquina "no viva" y se aprovecha su dirección *IP* para engañar a sus posibles emisores y para capturar información que vaya dirigida a ella.
  Este tipo de ataque se realiza desde dentro de las organizaciones (*intranets*) donde puede pincharse la red local sin mayores problemas.

- *sendmail spoofing*: Enviar *E-mails* conectándose al *port 25* desde el anonimato. Ese anonimato puede ser aprovechado para muy diversas fechorías.
- *DNS spoofing*: acceder a un servidor de *DNS* local y cambiar un nombre de máquina por otro para engañar a un *DNS* remoto, de forma que un ordenador recibe el tráfico dirigido a otro.

10 Soluciones a la inseguridad en *Internet* e *intranets*

Del mismo modo que los amigos de la información ajena han detectado las debilidades ya conocidas, los expertos informáticos trabajan también en la búsqueda de soluciones para las debilidades manifestadas en los sistemas informáticos.

10.1 SISTEMAS OPERATIVOS REFORZADOS (NIVEL C2 DE SEGURIDAD)

Como ya se ha indicado, el mínimo que debería exigirse a cualquier sistema multiusuario en la actualidad es *División C Clase 2* de seguridad que garantice que:

- Los *controles de acceso* deben poder identificar totalmente a los usuarios individualmente y dentro de los grupos a que pertenecen.
- *Accounting* (contabilidad) del sistema capaz de identificar claramente a todos los usuarios en el proceso de *login* (entrada) al sistema.

- Posibilidad de *auditar eventos* relevantes desde el punto de vista de la seguridad.
- *Aislamiento de los recursos*, tal que los objetos sean "borrados" antes de volver a ser reasignados a otros usuarios. Por ejemplo, borrar las zonas de memoria usada por un usuario antes de asignárselas a otro usuario.

10.2 COMUNICACIONES SEGURAS (IPV6 Y FIREWALLS):

Ipv6 la siguiente generación de *IP (IPng)*

Sin lugar a dudas, la mejor noticia para los sensibilizados con la seguridad en la *Red* es la aparición del nuevo protocolo *IP, IPv6* que hará realidad la seguridad en el *nivel de red* de *Internet.*

IPv4 presenta, actualmente, problemas de seguridad y carencias evidentes de mecanismos de *privacidad* y *autentificación* bajo la *capa de Aplicación.*

IPng intenta remediar todo esto con dos opciones integradas que ofrecen servicios de seguridad y que pueden usarse por separado, o conjuntamente, para ofrecer diferentes niveles de seguridad a usuarios con características propias.

El primer mecanismo de seguridad de *IPv6* es *"IPng Authentication Header"* cabecera de extensión que ofrece *autentificación* e *integridad (*sin *confidencialidad)* a los *datagramas IPng.*

Puede usarse para eliminar varios tipos de ataques de red incluido el *enmascaramiento de hosts.* Su inclusión en la *capa Internet* puede ayudar a ofrecer *autentificación de host origen* a los protocolos de capas superiores y a los servicios que actualmente carecen de protecciones.

Este mecanismo, además, es exportable fuera de EUA por no ofrecer la *confidencialidad* que ofrece el cifrado fuerte considerado un arma de guerra en Estados Unidos.

El segundo mecanismo de extensión de cabecera de seguridad de *IPng* es *"IPng Encapsulation Security Header"* que ofrece *integridad y confidencialidad* a los *datagramas IPng.* Usa cifrado *DES CBC* como algoritmo estándar para abarcar la globalidad de *Internet.*

Redes firewall (cortafuegos)

Consiste en uno o varios métodos de protección de una red segura de otra red no fiable. Existen en la actualidad muchas formas de enfrentarse a este tipo de protección, pero todos los *firewalls* pueden resumirse en un par de mecanismos: uno basado en bloquear el tráfico, y el otro consistente en permitirlo. Algunos *cortafuegos* ponen gran énfasis en bloquear el tráfico, mientras otros enfatizan su permisividad.

A grandes trazos, un *firewall* es cualquiera de las formas de proteger una red que desea asegurarse de otras redes de las que se desconfía.

Las técnicas de *cortafuegos* han comenzado a popularizarse al mismo ritmo que las *intranets*. Las organizaciones que optan por implantar *intranets* y conectar también con *Internet* comprenden rápidamente la necesidad de proteger su red de área local de los potenciales ataques que pueden acechar desde la inmensidad de *Internet*.

Algunos *firewalls* sólo permiten tráfico *E-mail* eliminando cualquier otra comunicación con el exterior de la corporación. Otros *firewalls* no son tan restrictivos impidiendo sólo el uso de *finger remoto*, o entradas *telnet* desde nodos sospechosos.

Los administradores de redes y los responsables de seguridad son los que deben decidir qué política aplicar al elegirlos. Si su organización necesita de los servicios de *Internet* pueden decidir actuar sobre sus *routers* para filtrar determinadas direcciones, impidiendo la entrada o salida a posibles infractores.

En cuanto al coste de los *firewalls* es importante destacar que puede ir desde varios millones, hasta 0 Ptas. si se eligen productos *freeware* existentes en la Red.

Funciones de los *firewall*:

- Cuidar la información que sale de una red privada corporativa a otra red insegura como puede ser *Internet* (***Figura 1***)
- Todo el tráfico que entra y sale de la organización debe pasar por el *firewall*.
- Sólo debe permitirse pasar el tráfico que está definido en la *política de seguridad*.
- El *firewall* debe autoprotegerse contra los ataques, pues debe ser la parte más protegida de la red, ya que es lo que se ve desde fuera de la organización.
- "*Lo que no esté expresamente permitido, está prohibido*" o...
- "*...lo que no está expresamente prohibido está permitido*". Es necesario buscar el punto de equilibrio entre estos dos planteamientos extremos en la definición de los *firewall*.

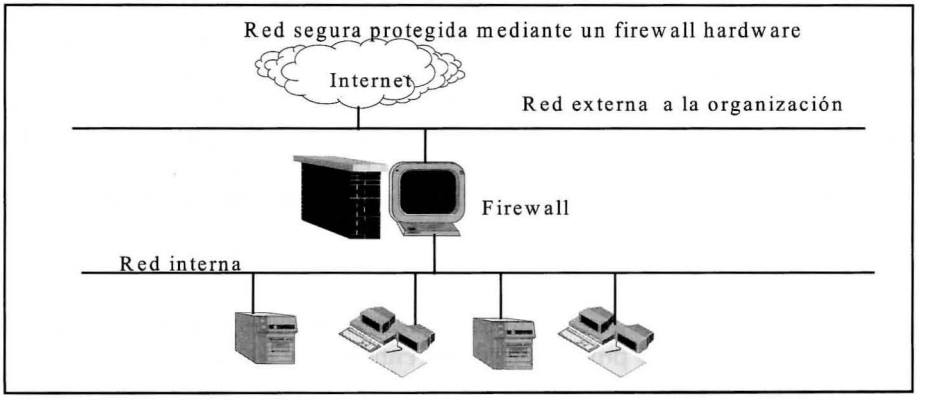

Figura 1 *Posición estratégica de los firewall*

10.3 USUARIOS CONCIENCIADOS

Los usuarios de *Internet* desde sistemas multiusuario deberían estar atentos a los siguientes puntos:

- Mensajes de *lastlog* (mensaje dado por el sistema sobre la última entrada al mismo).
- Cambios periódicos de sus *passwords.*
- No dejar sesiones abiertas.
- Cuidar los privilegios de sus ficheros.
- Concienciarse que, aunque no tengan nada importante en su cuenta de usuario, ésta puede ser usada para acceder al sistema y utilizarse para sabotear a otros usuarios con información valiosa.
- Política de elección de contraseñas según lo comentado anteriormente.
- Precaución ante los virus que pueden llegar desde la *Red.*
- En suma, mantenerse informados y alerta.

En cuanto a los usuarios de ordenadores personales, poco pueden temer de los ataques contra la información que almacenan. Los ataques se cometen contra la información depositada en los sistemas *servidores* o contra la información que viaja por las redes. Estos usuarios deben preocuparse más del acceso físico que del acceso lógico. Sobre todo deben cuidar la información que "bajan" de la *Red* para evitar los contagios víricos. Deben ser conscientes también que la información que envían a la *Red* puede ser capturada, por lo que deberán adoptar las medidas oportunas como es el uso de la criptografía que se explica en el siguiente apartado.

11 *Criptografía,"la clave"* para la *privacidad* de la información

Ante los ataques que puede sufrir la información cuando "viaja" a través de las demostradas inseguras redes, la solución más tranquilizadora para aquellos usuarios que necesiten transmitir información sensible es el *cifrado* de ésta. Lógicamente, el proceso de *encriptación* de la información es más incómodo que enviarla en *texto plano* sin ningún tipo de cifrado. Pero ha quedado ya demostrado que, en la actualidad, casi toda la información puede ser interceptada usando las técnicas que aquí se han comentado, por lo que el precio que se ha de pagar en tiempo para obtener esa necesaria privacidad creemos que está justificado.

Se presentan a continuación algunos conceptos relacionados con la *criptografía.*

Misiones de la criptografía:

Proporciona comunicaciones seguras a través de canales que no lo son, permitiendo la comunicación privada entre dos entidades y evitando que el mensaje sea comprendido por una tercera entidad que pueda estar a la *"escucha".* Permite también proteger información sensible archivada en ficheros y en los

backups realizados en soportes que puedan ser robados. Además, garantiza la protección de información si el sistema se ve comprometido. El *cifrado* de la información no impide los borrados de información, pero sí que ésta pueda ser tergiversada o comprendida por terceras personas.

En suma, la criptografía garantiza la *seguridad*, pero también la *privacidad* y la *autentificación* ya que permite el uso de *firmas digitales* para que el receptor de un mensaje pueda *certificar* la verdadera personalidad de su emisor.

Seguidamente se presenta brevemente la división clásica de criptosistemas que ya tienen su aplicación en *Internet*.

11.1 *CRIPTOSISTEMAS SIMÉTRICOS* O DE *CLAVE SECRETA*

Sólo las entidades usuarias de la *criptografía* conocen la clave que deben mantener en secreto para obtener la privacidad buscada.

La clave se genera por un determinado algoritmo que puede ser conocido o no.

DES (Data Encryption Standard) desarrollado por *IBM*, es el criptosistema de clave secreta más utilizado. Se basa en un algoritmo conocido de cifrado-descifrado de bloques de 64 bits que usa permutaciones mediante una clave de otros 64 bits.

Los *criptosistemas simétricos* tienen dos importantes inconvenientes:

- La clave secreta debe ser suministrada por el emisor al receptor cada vez que establecen una comunicación. Para ello puede usar el mismo canal de comunicación (la *Red*) u otro (teléfono por ejemplo). Pero esto produce ineficiencia e inseguridad, ya que si existiese algún canal seguro para transmitir la clave, ya no sería necesaria la criptografía.
- Puede intentarse la repetición del proceso de encriptación con el uso de diccionarios que es la técnica usada por los programas *cracker* ya comentados en este capítulo.

El emperador romano Julio César, ya en el año 70 antes de Cristo, usaba uno de los sistemas de clave secreta más simple y conocido. Cifraba sus mensajes secretos haciendo corresponder a cada letra del alfabeto el carácter situado en la posición ordinal inmediatamente menor del alfabeto. Así, la letra "a" la representaba como "z"; la "b" como "a"; la "c" como "b"; etc.. Éste ha sido el algoritmo aplicado para cifrar la frase que encabeza este capítulo y, como puede comprenderse, el inconveniente de este sistema de cifrado está en que, una vez conocido el algoritmo de cifrado, conocer el mensaje es inmediato.

11.2 *CRIPTOSISTEMAS ASIMÉTRICOS* O DE *CLAVE PÚBLICA*

Éstos son el mejor antídoto contra las técnicas de *sniffers* ya comentadas. Cada usuario dispone de un par de claves, una privada y otra pública. El originador del mensaje lo encripta con la clave pública del destinatario. El destinatario descifrará el mensaje con su propia clave privada que solo él conoce.

Un intruso (*sniffer*) que intercepte el mensaje no puede entenderlo a menos que conozca la clave privada del destinatario.

RSA (Rivest, Shamir y Adleman) es el más popular de estos *criptosistemas*. Las claves privada y pública se componen de un exponente y un módulo producto de dos números primos grandes para que su factorización sea inabordable en un tiempo aceptable para los ordenadores actuales. Así, difundir la clave pública no hace peligrar la privada.

Existen ya interesantes implementaciones de sistemas criptográficos pensados para conseguir la necesaria seguridad en la *Red* que van a ser comentados en el siguiente apartado dedicado al software de dominio público.

12 Software de dominio público orientado a la seguridad de los sistemas y servicios de *Internet*

La filantropía de los informáticos que han implementado software de dominio público, libre o gratis (*freeware*) poniéndolo a disposición de todo el que desee aprovechar su esfuerzo ha *"beneficiado"* también a la seguridad informática. Van a presentarse algunas de las más significativas herramientas *freeware* para garantizar una mayor seguridad de la información. No obstante, es imprescindible -y urge destacar- que la mayor parte del *freeware* que va a presentarse puede ser considerado como un arma de doble filo. Paradójicamente, y aunque la mayoría de los desarrollos se realizaron pensando en usuarios dignos de confianza, algunos pueden convertirse en auténticos misiles dirigidos a la línea de flotación de muchos sistemas o redes que están débilmente administradas, en cuanto a seguridad se refiere, si caen en manos de *hackers* o *crackers*.

No van a poder analizarse todos, pero nos centraremos en los dos que hemos considerado más útiles tanto para usuarios finales como para *administradores de sistemas y de comunicaciones*.

12.1 EL SISTEMA *KERBEROS*, EL CANCERBERO IDEAL PARA REDES INFORMÁTICAS SEGURAS

En 1983 el *MIT (Instituto Tecnológico de Massachusetts)* junto con *IBM* y *DEC* emprenden el proyecto *ATHENA* basado en la modelo *Cliente/Servidor* configurando la *MITnet*, la red de campus universitario del *MIT*.

Para reducir los peligros de inseguridad se implementó el *sistema de certificación Kerberos* para evitar el envío de contraseñas sin encriptar a través de las, siempre vulnerables, redes.

Kerberos es un sistema de autentificación para redes físicamente inseguras (casi todas), basado en un modelo de distribución de claves propuesto por *R.M. Needham y M. D. Schoroeder*. Posibilita la comunicación a través de red garantizando la identidad de las entidades que participan en la comunicación y previe-

ne las indiscreciones y ataques. También garantiza la integridad de datos evitando su detección y manipulación, y la privacidad, evitando las lecturas no autorizadas usando el sistema criptográfico *DES*.

Kerberos suele usarse en protocolos del nivel de *Aplicación (Nivel 7 del modelo OSI)* como *Telnet y FTP* para ofrecer seguridad desde usuario a *host*. Suele usarse también, aunque con menor frecuencia, como sistema de autentificación de datos *(SOCK, STREAM)* o mecanismos *RPC (Nivel 6 del modelo ISO)*. Incluso puede usarse a niveles bajos para seguridad de *host a host* con protocolos *IP, UDP* o *TCP (niveles 3* y *4 de ISO)*.

Características de la *MITnet:*

- Más de 10.000 ordenadores.
- Backbone de Fibra Óptica con ancho de banda de 100 Mbits/s.
- Más de 100 LAN's *Ethernet*.
- Más de 1.200 ordenadores forman parte de *Athena*.
- Cifra superior a los 25.000 estudiantes.

Los ingenieros informáticos del *MIT* eran conscientes de los siguientes puntos negativos en cuanto a la seguridad se refiere:

- Las grandes redes son, físicamente, inseguras (cableado difícil de proteger).
- Casi todas las redes son *broadcast* (difusión pública) y todo ordenador conectado a la red tiene acceso a toda la información que viaja por la red.
- Un intruso en la red puede hacer que le lleguen datos que no son para él e, incluso, suplantar la personalidad de otro usuario.

Para evitar los problemas anteriores se propuso el sistema *Kerberos* caracterizado en los siguientes puntos:

- Verifica y certifica los paquetes de datos que viajan por *Athena*.
- Sistema distribuido que usa un mecanismo de intercambio de información cifrada antes de permitir el acceso a los servidores.
- Realiza verificaciones criptográficas para garantizar que los datos transferidos entre estaciones de trabajo y servidores no se corrompan por accidentes o por accesos no autorizados.
- Utiliza el estándar *DES* para cifrar cada paquete de información mediante una clave que sólo conocen el *cliente* y el *servidor*, de forma que la información no tenga ningún valor para un tercero que pueda interceptar el mensaje.
- Si el atacante intenta modificar el contenido del mensaje, el destinatario solicitará el reenvío de los paquetes manipulados, y el interceptor quedará al descubierto.

Las claves de todos los usuarios y servidores son sólo conocidas por un *servidor* especial llamado *CDC (Centro Distribuidor de Claves)* que interviene en todas las transacciones usando *tickets digitales* de certificación, y que se encuentra en lo que en el *MIT* llaman *la mazmorra,* inaccesible sin autorización.

En cuanto a la situación legal de *Kerberos,* cabe decir que parece ser que siguen sin quedar claras las competencias de los *Departamentos de Estado* y *Comercio* estadounidenses. El *Departamento de Comercio* controla la exportación del software y hardware de *autentificación,* mientras el *Departamento de Estado* impide la exportación de material *criptográfico* fuera de USA. El problema, por tanto, está en encontrar la línea divisoria entre lo que realmente es *Kerberos,* un *sistema de autentificación* como parece evidente, o un *criptosistema* que usa *DES* considerado no exportable por el *Departamento de Estado.* Mientras esto queda claro, y para no infringir ninguna ley *Federal* lo que puede hacerse para testear esta potente herramienta es usar *Bones* que ofrece únicamente el *API* de *Kerberos* sin usar *encriptación* ni ofrecer seguridad.

Bones es una solución parcial al problema legal de exportación de material criptográfico fuera de USA. Mediante la definición de un símbolo en tiempo de compilación se evita usar las llamadas y librerías de *encriptación* de *DES* para poder transportar los fuentes entre fronteras de distintos países sin infringir ninguna ley Americana.

12.2 PGP PRETTY GOOD (TM) PRIVACY PARA EL CORREO ELECTRÓNICO SEGURO

Herramienta *freeware* ejemplo de *criptosistema* de *clave pública* que funciona sobre *MS-DOS, Windows, Mac, Unix* y *OpenVMS* entre otros sistemas operativos.

Puede usarse para *criptografía convencional* de información contenida en ficheros, aunque su utilidad principal es la de cifrar mensajes de correo electrónico.

Permite una gestión personal de anillos (ficheros) de claves públicas y privadas. Además, comprime la información lo que redunda en ahorro de tiempo en transferencias y en ocupación de espacio de disco.

Proporciona también autentificación de emisor con la posibilidad de usar *firmas digitales* que pueden ser certificadas por notarios o certificadores de firmas electrónicas.

Permite elegir entre módulos de 512, 768 ó 1024 bits en función de la complejidad de clave que desee obtenerse. Emplea el algoritmo *RSA* para la generación de claves públicas.

La ***Figura 2*** ilustra la forma de enviar mensajería cifrada a través de *Internet* usando *PGP.*

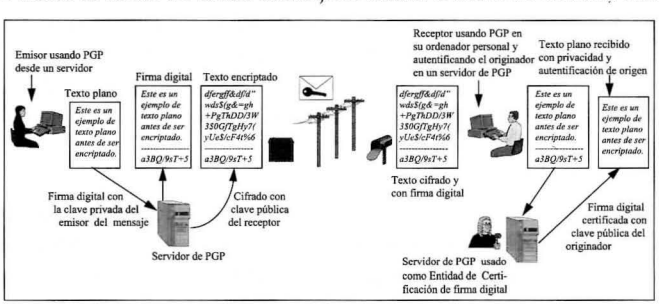

Figura 2 *Funcionamiento de PGP*

La ***Tabla 2*** presenta una relación de productos de dominio público orientados a la seguridad. La mayor parte de ellos están disponibles también en el servidor de *ftp anonymous* de *RedIRIS* (*ftp.rediris.es*) en el directorio */mirror/coast/tools/unix/**.

PRODUCTO	AUTOR(ES)	LOCALIZACIÓN
audit.	Bjorn Satdeva	gjorn@sysadmin.com
CAP	D. Thompson/K. Arndt	thompsond@orvb.saic.com
COPS	D. Farmer	ftp cert.org:/pub/tools/cops (192.88.209.5)
Crack	Alec Muffetf	ftp cert.org:/pub/tools/crack/crack_4_1.tar.Z
CrackLib	Alec Muffet	ftp cert.org:/pub/tools/cracklib
Etherwatch/Latwtach	David B. Sneddon	sneddo@perth.dialix.oz.au
Guess	Joe Meadows Jr.	http://www.wku.edu/www/fileserv/fileserv.html
HSC-Gatekeeper	Herve Schauer	Herve.Schauer@hsc-sec.fr
ISS	Chris Klaus	USENET comp.sources.misc y ftp cert.org:/pub/iss
Kerberos y Bones	MIT	ftp athena-dist.mit.edu:/pub/kerberos5 (18.159.0.42)
Kernel_wrap	CIAC, CERT, FIRST	ftp eecs.nwu.edu:/pub/securelib (129.105.5.105)
Miro	miro@cs.cmu.edu	ftp ftp.cs.cmu.edu (Proyecto Miro) (128.2.206.173)
Npasswd	Clyde Hoover	ftp ftp.rediris.es:/pub/soft/security (130.206.1.2)
One-time Password	cert@cert.org	cert@cert.org
Passwd+	Matt Bishop	ftp ftp.dartmouth.edu:/pub/security/passwd+.tar.Z
PGP	Philip Zimmermann	ftp://idea.sec.dsi.unimi.it (149.132.3.4)
Satan	W. Venema/ D. Farner	ftp ftp.caltech.edu:/caltech/security/satan (131.215.48.49)
SecureLib	William LeFevre	ftp eecs.nwu.edu:/pub/securelib.tar
Shadow	John F. Haugh III	comp.sources.misc:/usenet/comp.sources.misc/volume38
SOCKS	D. Koblas/M. R. Koblas	s1.gov:/pub/socks.tar.Z (128.15.32.7) y ftp.rediris.es
SPI	Gene Spafford	spaf@cs.purdue.edu o consultar CIAC
STEL	D.Vincenzetti/S.Taino	ftp://idea.sec.dsi.unimi.it
SUPERVISOR	Hunter Goatley	http://www.wku.edu/www/fileserv/fileserv.html
Swatch	CERT,FIRST	ftp://ftp.Stanford.EDU/general/security-tools/swatch
TAMU	Safford/Schales/Hess	ftp net.tamu.edu:/pub/security/TAMU (128.194.177.1)
TCP Wrapper	Wietse Venema	ftp cert.org:/pub/tools/tcp_wrappers/tcp_wrappers.*
TIS Firewall ToolKit	TIS	ftp ftp.tis.com:/pub/firewalls/toolkit (192.94.214.101)
TripWire	Kim/Spafford	ftp://coast.cs.purdue.edu/pub/COAST
Watcher	Matt Madisson	http://www.wku.edu:/www/fileserv/fileserv.html
Xwatchwin	George D. Drapeau	ftp ibmserv.edu.tw:/pub1/xwatchwin (140.111.3.11)
YPX	Rob Nauta	USENET comp.sources.misc y ftp.rediris.es

Tabla 2 *Relacción de Freeware orientado a la seguridad en INTERNET.*

13 Organizaciones públicas para velar por la seguridad mundial de redes y sistemas

Además del software de dominio público puesto amablemente a disposición de todos por sus desinteresados autores, existen también organizaciones que podríamos llamar de dominio o servicio público que, sin ningún afán de lucro, realizan una impagable labor como asesores ante episodios relacionados con vulneraciones a la seguridad de los sistemas informáticos de todo el planeta. Entre ellas destacan las siguientes.

13.1 CERT (COMPUTER EMERGENCY RESPONSE TEAM)

Ente de la *Universidad de Carnegie Mellon* que actúa como asesor ante incidentes relacionados con la seguridad de la información. Periódicamente informa sobre todo lo relacionado con problemas de inseguridad (*bugs* en protocolos y sistemas, ataques, estadísticas, etc.). No tiene fuerza legal pero sí autoridad reguladora. Atiende consultas las 24 horas del día en el Tel. +1 412 268-7090 y man-

tiene también valiosísimas listas de distribución de correo electrónico como *cert-advisory-request@cert.org.*

13.2 CIAC (COMPUTER INCIDENT ADVISORY CAPABILITY)

Soportado por el *Departamento de equipos de energía de Lawrence Livermore National Laboratory.* Desarrolla líneas de acción para responder ante incidentes, e implementa software para responder a eventos relacionados con inseguridad. Informa, forma, alerta y asiste a organizaciones que han sufrido ataques.
Teléfono +1 510 422-8193. *E-mail: ciac@lln1.gov*

Existen otras organizaciones que ofrecen un servicio similar como son:

- *NIST (National Institute of Standards and Technology).*
- *FIRST (Forum of Incident Response and Security Teams).*
- Además, organizaciones españolas como *RedIRIS*, entre otras, disponen de su propio *CERT-ES* ofreciendo los servicios del *CERT* original con un ámbito local (*cert@rediris.es).* En España existe también *esCERT* para apoyo privado.

14 Seguridad en *WWW* para el comercio electrónico seguro.

Podría decirse que, en el contexto de la seguridad en *Internet*, se establecen dos grandes divisiones, *seguridad en general* y *seguridad para las transacciones financieras.* En el primer grupo pueden situarse la mayor parte de las herramientas citadas hasta este momento. En el segundo grupo podemos enmarcar la mayoría de soluciones que, a modo de nota, se exponen seguidamente y que deben tenerse en cuenta para entender la inquietud existente en la actualidad en torno al tema de la seguridad en la telecompra a través de *Internet.*

- *Mastercard* y *Visa* han firmado un acuerdo para desarrollar la especificación *SET (Secure Electronic Transactions)* basada en encriptación *RSA. SET* podría convertirse en un estándar internacional gracias al apoyo de *ISO.*

- *Netscape, Microsoft* e *IBM* están detrás de *SSL (Secure Socket Layer),* protocolo que define la comunicación segura entre aplicaciones *clientes* y *servidoras.* Utiliza algunas variedades de algoritmos de encriptación estándares como *DES* y *RSA* con claves de 40 ó 128 bits. *Netscape* ha propuesto su versión 3.0 de *SSL* como *Internet Draft* al *IETF* para que éste lo certifique como estándar.
  Además, *Netscape* ha anunciado *Secure Courier* para encriptar datos específicamente financieros como son los números de tarjetas de crédito enviados a través de la *Red.*

- *Terisa Systems* ha *desarrollado S-HTTP (Secure HTTP),* un conjunto de protocolos para conseguir *confidencialidad, integridad* y *autentificación* espe-

cíficamente en transacciones *HTTP*. Empiezan a extenderse los servidores de *WWW* cuyo *URL* comienza con *https://* pensados para el envío de información confidencial o para realizar transacciones financieras seguras a través del *W3*.

- El *CERN* trabaja en *Shen*, un conjunto de extensiones de seguridad también para el protocolo *HTTP*.

- Otro reciente desarrollo, son los *RFC 1825-1829*, para tener protocolos efectivos de cifrado o autentificación de tráfico en *IP*. Se está profundizando aún más en la gestión de claves, y todo esto desembocará, antes o después, en herramientas para conexiones de red autentificadas sobre una filosofía abierta como la de *Internet*.

- El cuarto programa marco de *UE* ha puesto en marcha el proyecto *ICE* que persigue, entre otras cosas, establecer una jerarquía de certificación inspirada en la misma base estándar usada en *PEM* y *MOSS* que son dos protocolos estándarizados por el IETF y pensados para la seguridad de la mensajería electrónica.

- Una vez especificada e implementada la arquitectura de seguridad y los mecanismos para obtener la autentificación y privacidad propuesta por *IPv6*, quedaba por adoptar el protocolo que se encargase de gestionar las claves criptográficas de las firmas digitales que están empezando a extenderse ampliamente en *Internet*. El protocolo adoptado para esa gestión de claves ha sido *ISAKMP/Oakley*.

Todas las soluciones que acaban de enumerarse giran en torno al cifrado de la información generada en las transacciones financieras y electrónicas. Pero no sólo se han encontrado soluciones en la criptografía, existen otros métodos de realizar operaciones comerciales seguras como los expuestos en el apartado 5 del *Capítulo 17*, donde se comentan *Digicash* y *Firts Virtual Bank*. Existen además otras soluciones similares como *Cybercash*, *First Data* y *SEPP* (*Secure Electronic Payment Protocol*).

La enumeración de novedades relacionadas con la seguridad en *Internet* es ciertamente difícil por su extensión. Seguidamente (***Tabla 3***) se incluye una relación de *URLs* de organizaciones comerciales y públicas relacionadas con el tema para aquellos lectores interesados en seguir más de cerca esta importante faceta de la *Red*.

Organización	URL
Anyware Seguridad Informática	http://www.anyware.com
ASLAN	http://www.aslam.es
Authentex	http://www.authentex.com
CERT	http://www.cert.org
CERT Rediris	http://www.rediris.es/cert
Encryption Policy Resource Page	http://www.crypto.com
EPIC	http://www.epic.org
ES-CERT	http://escert.upc.es/castella/cert.html
FIRST	http://www.first.org/first
FTP software	http://www..ftp.com
Internet Privacy Coalition	http://www.privacy.org/ipc
Internet Security Systems	http://www.iss.com
Iworld	bbs.seker.es/valvy/crypto.html
McAfee	http://www.mcafee.com
Pretty Good Privacy	http://www.pgp.com
RSA	http://www.rsa.com
Security in Computing and Communication	http://www.sc2.es
Sinutec	http://www.sinutec.es
The World Wide Web Security FAQ	http://www.w3.org/Security/Faq
TRUSTe	http://www.truste.org
Trusted Information Systems	http://www.tis.com
Verisign	http://www.verisign.com

Tabla 3 *Organización relacionadas con la seguridad*

De las anteriores referencias queremos destacar especialmente *http://www.w3.org/Security/Faq,* que posee un *mirror* en España en el *URL http://www.uniovi.es/~rivero/mirror/www-security-faq,* que se encargan de mantener actualizadas las *FAQs* sobre seguridad en *WWW.* En cualquiera de esas dos referencias puede obtenerse información precisa sobre los múltiples agujeros de seguridad que aquejan a *Web,* ya sea en los *browsers,* en los propios *servidores,* o por problemas encontrados en los programas *CGI, JavaScript, applets de Java* y controles de *ActiveX.*

Además, puede ampliarse información sobre cualquiera de los temas comentados en este capítulo en las siguientes referencias de la *Red.*

- En primer lugar, son de interés las *FAQs* sobre criptografía que pueden encontrarse en el grupo de noticias *sci.crypt,* y la *FAQ* sobre privacidad y anonimato del grupo *news.asnswers.*

- *APEDANICA (Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas)* mantiene la lista de distribución *apedanica@encomix.es*

- Lista de distribución sobre *firewalls*: *majordomo@greatcircle.com* (Enviar mensaje indicando *subscribe firewalls*).

- Son de interés también los siguientes grupos de *News* relacionados con el tema: *alt.hackers, alt.politics.org.nsa, alt.privacy.*, alt.security.*, comp.risks, comp.society.privacy, comp.security.announce, sci.crypt* y *talk.politics.crypto.*

15 Conclusiones

Han quedado patentes las debilidades relacionadas con la seguridad que los sistemas informáticos padecen. Los usuarios de *Internet* pueden verse afectados por esas debilidades, pero existen importantes soluciones y a coste cero si se emplea la gran cantidad de *freeware* existente en la *Red*. Tanto los administradores de comunicaciones y sistemas como los usuarios finales tienen en sus manos la solución a los problemas de inseguridad provocadas por las sibilinas técnicas de violación de información que se han popularizado en poco tiempo.

Las estadísticas del *CERT* indican que casi el 100 % de los ataques provienen de los *sniffers* y programas *crackers* de contraseñas. Los *sniffers* pueden ser detectados y los *crackers* no se atreven con *passwords* bien elegidas. Además, cuando realmente se maneje información confidencial, puede optarse por la criptografía. El problema de las infecciones víricas transmitidas a través del correo electrónico puede ser contrarestado con las debidas precauciones.

El incipiente comercio electrónico cuenta ya con importantes y variadas soluciones para que la inseguridad no impida su desarrollo con esa enorme potencialidad que a nadie se le escapa. Estas importantes perspectivas económicas están provocando que la mayor parte de gobiernos del mundo tomen iniciativas para conseguir tecnologías y servicios seguros y fiables en torno al comercio electrónico, así como las necesarias medidas legales que contemplen la virtualidad de las fronteras que Internet posibilita.

Estamos ante un problema preocupante, pero no hemos de caer en situaciones de psicosis general, sino en la oportuna concienciación ya que debilidades existen, pero como hemos tenido ocasión de comprobar también soluciones para evitarlas. Hemos de tener bien presente que la Red es en estos momentos la herramienta de comunicación más poderosa que existe y resulta difícil encontrar el punto de equilibrio entre facilidad de uso y seguridad. En cualquiera de los casos, Internet es mucho más segura que cualquiera