ETSIT UPM

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

Isdefe

Cuadernos Cátedra ISDEFE-UPM

5

Seguridad en redes de telecomunicación

Víctor A. Villagrá González

Seguridad en Redes de Telecomunicación

Víctor A. Villagrá González

Con la colaboración y revisión de:
Verónica Mateos Lanchas
Grupo de Redes y Servicios de Telecomunicación e Internet
Departamento de Ingeniería de Sistemas Telemáticos
E.T.S.I. de Telecomunicación-UPM

Primera edición: Abril 2009

Edita:
Fundación Rogelio Segovia para el
Desarrollo de las Telecomunicaciones
Ciudad Universitaria, s/n
28040-Madrid

Imprime:
E.T.S.I. de Telecomunicación
Universidad Politécnica de Madrid
Ciudad Universitaria, s/n
28040-Madrid
Diseño de cubierta y
maquetación: Rocio Ortega

ISBN (13): 978-84-7402-356-5
ISBN (10): 84-7402-356-4
Depósito Legal: M-14404-2009

Índice

Presentación

La espectacular evolución de las tecnologías de la información y las telecomunicaciones ha permitido que, en los últimos años, hayamos asistido a un desarrollo sin precedentes de los servicios que proporcionan a los ciudadanos, permitiendo el incremento exponencial de los volúmenes de información intercambiados y posibilitando además el acceso a los mismos desde cualquier parte del mundo (incluso en movilidad cuando nos trasladamos de una ubicación a otra), habilitando lo que se ha dado en llamar la Sociedad de la Información.

Sin embargo, este rápido progreso ha exigido como compensación el pago de un precio muy alto, como lo constituye la aparición de nuevas vulnerabilidades y amenazas que elevan de manera exponencial el nivel de riesgo al que se encuentran sometidas las infraestructuras de la información. Por ello, se hace necesario que sus medidas de protección evolucionen de manera similar, para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la integridad y la disponibilidad de las propias redes y sistemas que la manejan.

En este contexto se enmarca la presente monografía de la Cátedra Isdefe de la Universidad Politécnica de Madrid (UPM), que en esta nueva edición se centra en analizar la Seguridad de las Redes de Telecomunicaciones, conscientes como somos de que divulgar el conocimiento es la mejor manera de fortalecer el eslabón más débil de la cadena de la seguridad de la información, que siempre está constituido por las personas.

Tras enmarcar los conceptos básicos sobre los que se cimienta la seguridad de la información (activos, amenazas, vulnerabilidades, impactos, riesgos, …), relacionándolos entre sí para dar lugar al ciclo de vida de la propia seguridad, la presente obra se centra en examinar con detalle las Amenazas en Internet, la "Red de Redes", como no podría ser de otra forma para ser fieles al título del libro, haciendo un interesante análisis del perfil psicológico de los atacantes que se mueven en este medio.

A continuación, y para dar al lector las herramientas de protección adecuadas, se exponen los mecanismos que permiten un Acceso Seguro a la Red, descritos con detalle en dos grandes apartados, el de Autenticación y Autorización y el de Defensa Perimetral, profundizando en su tipología, en sus arquitecturas subyacentes y en los detalles tecnológicos de los sistemas que los implementan. A este respecto, y para los lectores habituales de la serie de monografías sobre seguridad de la Cátedra Isdefe-UPM, se incluye un epígrafe sobre Sistemas de Autenticación Biométrica, área tecnológica de una enorme y prometedora evolución, y cuyo estudio

ya fue abordado en profundidad por una edición anterior de la presente serie de monografías.

Por último, merece la pena reseñar el esfuerzo que se realiza al final de la obra para catalogar Empresas, Instituciones y Grupos de I+D, así como los principales proyectos e iniciativas del 7º Programa Marco de la UE, relacionados con la Seguridad en Red, como contribución para identificar actores e intereses de este nuevo sector de la seguridad TIC en constante evolución.

Finalmente, sólo nos queda felicitar tanto a los responsables de Isdefe como de la Universidad Politécnica de Madrid por esta nueva publicación puesta al alcance del público en general, lo que constituye un nuevo y exitoso hito en la colaboración de ambas instituciones para divulgar la cultura de la seguridad, como camino para poner a disposición de todas las personas los beneficios de la Sociedad de la Información.

D. Ignasi Nieto Magaldi
Vicepresidente Ejecutivo
Isdefe

Capítulo 1

Introducción

1. Introducción

El diseño y despliegue masivo de redes de telecomunicación acaecido en las últimas décadas, ha permitido la utilización de dichas redes a gran escala en la sociedad, convirtiéndose en piezas claves para el funcionamiento de empresas y administraciones, incluso a nivel individual, donde muchas personas ya no pueden imaginar una sociedad sin teléfonos móviles o Internet. La gran penetración social que están teniendo estas tecnologías ha hecho, a su vez, que se consideren muy especialmente como un potencial medio para la transmisión y ejecución de ataques contra los sistemas y los usuarios.

Si bien en las redes de telefonía este tipo de incidentes no es muy frecuente, la versatilidad de las redes abiertas de comunicación de datos hace que sea mucho más sencillo para los atacantes encontrar mecanismos en dichas redes que permitan llevar a cabo ataques. Aunque la existencia de riesgos e incidentes está presente en muchos entornos de comunicaciones de datos, el caso más significativo actualmente es el entorno de Internet, debido a su volumen, expansión y penetración social actual.

Los mecanismos básicos en los que se fundamenta Internet fueron diseñados durante la década de 1980 con el objetivo de intercomunicar centros de investigación y universidades, sobre todo en EE.UU. Este diseño no se realizó teniendo en cuenta la situación actual de uso a nivel mundial, sino que se hizo pensando en su utilización en entornos mucho más restringidos y sobre todo, pensando en usuarios con cierto nivel técnico y desde luego, no hostiles. Esto provoca que las tecnologías de seguridad que se incluyeron en los protocolos y servicios básicos de Internet en sus inicios, sean en la actualidad muy limitadas o incluso inexistentes en muchos casos.

El 2 de Noviembre de 1988, Robert Morris Jr., un estudiante de doctorado de informática de Cornell, desarrolló un programa experimental que aprovechaba una de las múltiples vulnerabilidades de los protocolos de Internet para autoreplicarse y autopropagarse a sistemas vecinos a través de Internet [1]. Lo lanzó desde el MIT, y rápidamente descubrió que se replicaba e infectaba las máquinas a una velocidad mucho mayor de lo que él esperaba, provocando la indisponibilidad de muchas máquinas en Internet por caída del sistema operativo o una evolución a un estado de inestabilidad en el que no era factible la ejecución de programas. Afectó a ordenadores de múltiples ubicaciones, incluyendo universidades, organismos militares e institutos de investigación médica. Este ataque, denominado el "Gusano de Internet (Internet *Worm*)" [2], fue la primera prueba de la falta de seguridad de los mecanismos básicos y protocolos de

Internet. El problema fue que ya era demasiado tarde para rediseñarlo de nuevo, por lo que continuamente se descubren nuevas vulnerabilidades en Internet, y es necesario desarrollar nuevos parches para cubrir dichas vulnerabilidades. En los últimos años este flujo de vulnerabilidades se acentuó debido a la aparición de vulnerabilidades, no sólo en los mecanismos de Internet, sino también vulnerabilidades de programación informática cometidas y detectadas en los programas encargados de implementar dichos mecanismos.

Ante estos hechos, ha sido necesario el desarrollo de distintas tecnologías especializadas en la seguridad en redes de telecomunicación, destinadas a proteger a los sistemas frente a diversos tipos de ataques, permitiendo el despliegue de arquitecturas de seguridad en red que facilitan el uso de las redes de una forma más segura y confiable.

Actualmente, el entorno de seguridad en las redes de telecomunicación se ha estabilizado después de muchos años convulsos, en los que era frecuente encontrarse con titulares de noticias relacionadas con nuevas vulnerabilidades encontradas en los medios de comunicación tradicionales. La tecnología ha madurado en cuanto a la sensibilidad sobre la seguridad informática, y el ritmo de aparición de vulnerabilidades ha decrecido en los últimos años.

No obstante, se trata de un entorno muy dinámico en el que los ataques se modifican muy frecuentemente, tanto en la forma como en el fondo. Hoy en día, los ataques buscan un beneficio económico en lugar de una relevancia mediática, y resultan más importantes aspectos como el correo electrónico no deseado generados por redes de ordenadores domésticos infectados, que las intrusiones producidas en ordenadores de organizaciones.

En este cuaderno se repasarán los principales mecanismos y tecnologías involucradas en la seguridad en redes de telecomunicación, desde el punto de vista del control de acceso a las redes para permitir una defensa frente a los posibles ataques.

1.1 Planificación de la Seguridad

En primer lugar, antes de analizar los aspectos técnicos de la seguridad en redes de telecomunicación y las tecnologías de seguridad relacionadas, es conveniente repasar algunos aspectos de planificación y organización que resultan relevantes para afrontar una estrategia de seguridad en redes de telecomunicación. Este tipo de planificación debe encuadrarse en una estrategia integral de protección de los sistemas de información de una

organización, y existen distintas normas y recomendaciones que permiten implantar, administrar, mantener y verificar una política de seguridad en sistemas de información. Este texto se centra solamente en uno de los aspectos más importantes de esta planificación: el análisis de riesgos.

1.1.1 Ciclo de seguridad

La planificación de seguridad puede ser descrita de forma general como un flujo de procesos destinados a la realización de un análisis de riesgos final, en lo que se denomina ciclo de seguridad [3], descrito en la Figura 1:

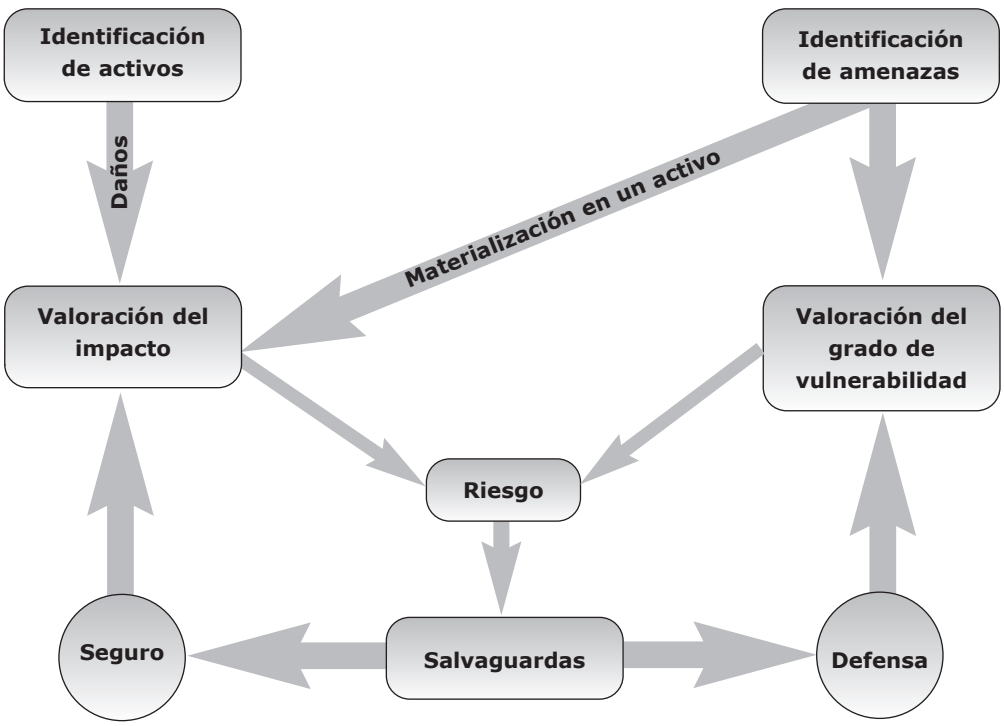

Figura 1: Ciclo de seguridad del proceso de planificación de seguridad

El ciclo de seguridad básico consta de varias fases:

- Identificación de los activos de la organización susceptibles de ser atacados. Se distinguen múltiples tipos de activos, tales como equipos, utilización de recursos, prestigio e imagen, etc.

- Identificación de las amenazas que podrían realizarse sobre dichos activos, desde amenazas por efectos atmosféricos o medioambientales, hasta amenazas más técnicas como puede ser un ataque desde redes externas.

- Valoración del impacto que una amenaza puede tener en un activo en caso de materializarse.

- Valoración de la vulnerabilidad del activo a dicha amenaza.

La combinación de vulnerabilidad e impacto de un potencial ataque define el grado de riesgo que se está corriendo ante dicho ataque. Un análisis de riesgos tiene como objetivo identificar estos riesgos y ser capaces de clasificarlos en función de su grado. Para los riesgos más peligrosos, se debe definir una política de seguridad con un conjunto de salvaguardas destinadas a disminuir por un lado la vulnerabilidad (actuación defensiva) y por otro el impacto de un posible ataque (actuaciones de seguro).

1.1.2 Activos

Se considera un activo todo aquello que usa o posee una organización y que es susceptible de ser atacado. En un entorno de sistemas de información y redes de telecomunicación existirán activos tales como:

- Recursos físicos, que tienen un valor económico en sí mismos.

- Utilización de recursos, ya que un ataque que atente contra la utilización de los recursos tiene un determinado impacto, bien sea por falta de disponibilidad o por pago por utilización.

- Información almacenada en los sistemas de información de la organización independientemente de la naturaleza de la misma (datos, software, etc.).

- Información en tránsito. Este activo, específico en los entornos que utilizan redes de telecomunicación, es el único que puede estar localizado en entornos externos al ámbito de una organización ya que

por información en tránsito se consideran los datos de la organización que están siendo transmitidos a través de redes externas a la organización. Esta información necesita unos mecanismos de protección distintos al resto; mientras que los activos localizados en el interior de la organización pueden ser objeto de mecanismos de defensa (evitar que el ataque llegue al activo), para estos activos sólo se pueden aplicar mecanismos de seguro (minimizar el impacto del ataque).

- Imagen de la organización. Este activo es de suma importancia en ciertos casos, ya que un ataque a la imagen de una organización puede ser publicitado en medios públicos, y la reputación de tal organización quedaría en entredicho, ocasionando unos costes indirectos que pueden ser cuantiosos.

- Personal y recursos humanos. Este activo debe estar en cualquier planificación de seguridad, aunque en el ámbito de la seguridad en redes de telecomunicación existen muy pocos ataques cuyo objetivo sean las personas.

1.1.3 Amenazas

Una amenaza es cualquier evento que puede desencadenar un incidente en la organización, produciendo daños en sus activos. La identificación de amenazas se puede hacer según su origen o según el activo objetivo de estas amenazas.

Según el origen, se pueden clasificar en amenazas originadas en el entorno (comunes a cualquier análisis de riesgos que conlleve recursos físicos, tales como amenazas climatológicas, ambientales, suministro eléctrico, etc.) y amenazas originadas por personas. Dentro de este último tipo de amenazas, se distingue a su vez entre amenazas de personal interno malintencionado, errores de personal interno y amenazas de personas externas malintencionadas.

Aunque las amenazas más famosas en el entorno de Internet y las redes abiertas de telecomunicación son las producidas por personal externo que intenta entrar en los sistemas de una organización, son mucho más peligrosas las amenazas del personal interno malintencionado. El motivo radica en que para defenderse del exterior es posible desarrollar tecnologías que bloqueen o filtren estas amenazas, pero es mucho más complicado impedir potenciales ataques del personal interno, ya que este personal tiene acceso a todos los recursos de la organización, siendo más difícil su detección y bloqueo. Existen formas de mitigar el problema, como el uso

de sistemas de autenticación y autorización de acceso a recursos internos por parte del personal de la empresa, así como la utilización de registros de toda la actividad, pero aún así, existe un determinado perfil de personal que podría, en un momento dado, evitar o anular dichos sistemas: los propios administradores de seguridad. Este perfil es muy sensible dentro de una organización, por lo que es necesario tener un seguimiento en detalle de estas personas, en cuanto a su predisposición a realizar ataques a los sistemas de la organización. Se requieren políticas de recursos humanos, promociones, etc. para este perfil de personal, mucho más específicas que para el resto de personal.

Por último, cabe destacar como potencial amenaza los propios errores del personal interno que, sin intención, pueden ser capaces de destruir o modificar activos del sistema. Como medida preventiva de este tipo de amenazas, es necesario incluir los adecuados sistemas de autenticación y autorización, así como unos métodos de recuperación de activos apropiados.

Hasta ahora, se han revisado las distintas amenazas existentes desde el punto de vista del origen de las mismas. Se detallan a continuación las amenazas más importantes en función de los activos objetivos:

- Amenazas a recursos físicos.

- Amenazas a la utilización de recursos.

- Amenazas a la información almacenada.

- Amenazas a la información en tránsito.

- Amenazas a la imagen y reputación.

- Daños a terceros.

1.1.3.1 Amenazas a recursos físicos

Las amenazas que pueden afectar a los recursos físicos son las mismas que en cualquier otro entorno de seguridad, como seguridad civil, seguridad del hogar, etc. Estas amenazas pueden ser:

- Amenazas intencionadas producidas por personas malintencionadas: robo, alteración, destrucción de equipos y sistemas informáticos.

- Amenazas de entorno: desastres naturales (inundaciones, terremotos, etc.), incendio, suministro eléctrico, temperatura, etc.

Las medidas de seguridad para este tipo de amenazas deben basarse en:

- Sistemas de control de acceso físico, para evitar el acceso de personal no autorizado a los recursos físicos.

- Sistemas de detección y prevención contra incendios, suministro eléctrico (sistemas de alimentación ininterrumpida), etc.

Sin embargo, es necesario ante este tipo de amenazas, desarrollar un denominado Plan de Contingencia [4] de la organización, que permita establecer los procedimientos de actuación para minimizar las consecuencias y el impacto de este tipo de amenazas.

1.1.3.2 Amenazas a la utilización de recursos

Como se ha comentado, la utilización de los recursos es un activo importante de una organización que puede ser atacado causando un cierto impacto. Las amenazas son frecuentemente provocadas por personas (internas o externas), que efectúan una utilización inadecuada de los recursos de la organización. Ejemplos de estas amenazas pueden ser los denominadas programas "*dialer*" que utilizan la conexión telefónica de la organización para llamar a números de tarificación elevada.

Las consecuencias de este tipo de amenazas se plasman en una reducción de disponibilidad de los recursos, y/o una pérdida económica cuando la utilización de los recursos implique un coste económico.

1.1.3.3 Amenazas a la información almacenada

Otro activo objeto de amenazas es la información de la organización, bien sean datos o programas almacenados en los discos o sistemas de almacenamiento. El impacto es mayor, normalmente, cuando se produce un ataque a los datos, pero no hay que desdeñar el impacto del ataque al software y a las aplicaciones, ya que suele suponer pérdidas de tiempo para la reinstalación de los sistemas. Existen distintos tipos de amenazas a tener en cuenta, como son:

- Ataques a la confidencialidad de la información, cuando el daño surge de desvelar el contenido de la información.

- Ataques a la integridad de la información, cuando el ataque modifica de alguna manera la información.

- Ataques a la disponibilidad de la información, cuando el ataque borra la información.

1.1.3.4 Amenazas a la información en tránsito

La información en tránsito es otro activo que hay que proteger. El factor diferenciador de este activo es que se trata de información de la organización que está en tránsito por redes externas sobre las que no se tiene control para implantar salvaguardas de tipo físico. Por lo tanto, todas las medidas de seguridad estarán orientadas a minimizar el impacto de este ataque, ya que es imposible llevar a cabo medidas de tipo defensivo. Los ataques que pueden darse son:

- Acceso al contenido de la información en tránsito (ataque a la confidencialidad).

- Modificación en tránsito del contenido de la información (ataque a la integridad).

- Introducción en tránsito de información falsa (ataque a la autenticación).

- Eliminación de datos (ataque a la disponibilidad).

Partiendo de los ataques anteriores, existen otros tipos de ataques específicos de la información en tránsito, que son los denominados ataques de repudio, los cuales se fundamentan en realizar una transmisión o recepción de datos, y negarlo posteriormente. Existen dos variantes de este tipo de ataques:

- Repudio de transmisión: negación de haber enviado datos alegando un ataque de autenticación (no lo transmití, alguien ha debido falsificar mi identidad para enviar esos datos).

- Repudio de recepción: negación de haber recibido datos alegando un ataque de disponibilidad (no lo recibí, alguien ha debido eliminar los datos antes de que llegaran).

1.1.3.5 Amenazas a la imagen y reputación

Las amenazas a la imagen y reputación de una organización son unas de las más extendidas actualmente por su facilidad relativa de realización. Son ataques que suponen un impacto pequeño en otros activos, pero un gran impacto por la pérdida de credibilidad y reputación que supone la

publicidad de estos hechos a gran escala.

Es uno de los ataques más frecuentes actualmente en Internet y se basa precisamente en la publicidad posterior del ataque, aunque éste no hubiese producido ningún impacto de consideración en los activos de la organización. Pero simplemente, el hecho de que se conozca a gran escala que la organización fue objeto de un ataque supone un perjuicio considerable para la imagen y la reputación de la organización. Incluso para determinadas tipos de empresas, como fabricantes de tecnología de seguridad, estos hechos podrían suponerle una grave crisis, ya que se menoscaba la credibilidad de su principal línea de negocio.

1.1.3.6 Daños a terceros

Por último, existen amenazas que no están dirigidas contra ninguno de los activos de una organización, que consisten en la utilización de los recursos de una organización para efectuar daños a terceros. De esta forma, organizaciones que no tienen unas adecuadas medidas de seguridad pueden ser convertidas en pasarelas de ataques a otros destinos, pudiendo ser objeto posterior de una posible petición de responsabilidades por los daños realizados.

Este es el caso de las denominadas redes de *bots* (*botnets*), que se esparcen accediendo a sistemas informáticos sin las adecuadas medidas de seguridad y desde ellos realizando diversas acciones, como por ejemplo, envío de publicidad no solicitada, participación en un ataque masivo de negación de servicio distribuido, etc.

1.1.4 Vulnerabilidades e impacto

El siguiente paso en un análisis de riesgos es la valoración de las vulnerabilidades específicas de la organización a las amenazas identificadas, y de los impactos que dichas amenazas pueden producir en los activos de la organización.

Se trata de una tarea muy compleja y muy específica de cada organización, por lo que es complicado dar unas pautas globales para efectuar dichas valoraciones:

- La vulnerabilidad debe medir de alguna forma la posibilidad real de que una amenaza se materialice sobre un activo de la organización. Este hecho depende de muchos factores globales y específicos de la organización, como su visibilidad global, su percepción por los usuarios, etc.

- El impacto debe medir las consecuencias de la materialización de una amenaza sobre un activo de la organización. En algunas ocasiones, se puede imputar una cuantía económica, pero la mayoría de las veces el impacto tiene componentes subjetivos específicos de la organización y del momento, como por ejemplo, una interrupción de un servicio, una publicitación de un incidente en medios de comunicación, etc.

Se trata de elementos muy difíciles de estimar cuantitativamente, por lo que es necesaria muchas veces una cuantificación relativa. Para un análisis de riesgos lo importante es conocer que se es más vulnerable a una cierta amenaza que a otra, o que un ataque tiene más impacto que otro. Este grado de cuantificación relativa para las vulnerabilidades y los impactos pueden ser suficientes para abordar un análisis de riesgos.

La valoración y cuantificación de la vulnerabilidad y los impactos y su posterior aplicación en el análisis de riesgos puede ser realizada mediante metodologías de análisis de riesgos. En el marco español, es muy utilizada la metodología del Consejo Superior de Administración Electrónica del Ministerio de Administraciones Públicas, denominada MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) [5].

1.1.5 Identificación de riesgos

El objetivo principal del análisis de riesgos es la identificación de riesgos para aplicar una política de seguridad optimizada para dichos riesgos. Para ello, es necesario identificar los riesgos a los que está sujeta la organización y que se deducen de los pasos anteriores al valorar las vulnerabilidades y los impactos.

Un riesgo representa una amenaza que puede materializarse sobre un activo y que se caracteriza por el grado de vulnerabilidad a la amenaza y por el impacto que supondría el ataque. La combinación vulnerabilidad - impacto es el grado de importancia de un riesgo, y cuanto mayor sea el impacto y más vulnerable se sea a un riesgo, más importante será el riesgo. Los peores riesgos son aquellos a los que se es muy vulnerable y suponen un gran impacto. Este hecho introduce una ordenación de los riesgos según su importancia, tarea clave a la hora de diseñar una política de seguridad, ya que la política de seguridad deberá concentrarse en los riesgos más importantes en primer lugar, dejando los riesgos menos importantes para segundo plano. El primer objetivo del análisis de riesgos es conseguir una tabla de riesgos ordenada según la importancia del riesgo,

determinada por la combinación de los factores vulnerabilidad e impacto del riesgo de acuerdo a alguna metodología.

Una vez elaborada la tabla ordenada de riesgos, el siguiente paso es decidir qué riesgos van a ser asumidos por la política de seguridad de la organización, es decir, cuales son los riesgos para los que se van a diseñar contramedidas basadas en soluciones tecnológicas o administrativas.

Por supuesto, la elección de riesgos empezará por el principio de la tabla de riesgos, afrontando en primer lugar los riesgos más importantes y continuando por los riesgos menos importantes del resto de la tabla de riesgos. Pero llegará un momento en el que será necesario parar, ya que no es económicamente rentable afrontar todos los posibles riesgos de una organización, puesto que el coste de afrontar el riesgo puede ser mayor que el coste que conlleva el impacto del riesgo. No hay que olvidar que la implantación de políticas de seguridad en las organizaciones tiene un coste elevado que hay que incluir en la planificación.

Los costes de la seguridad pueden ser:

- Costes directos, provocados por la instalación, implantación y operación de procesos y tecnologías de seguridad. En estos costes deberán estar incluidos las inversiones en nuevos equipos, sistemas, software, etc., así como su amortización, mantenimiento, operación y los gastos de personal específicos dedicados a la seguridad.

- Costes indirectos, provocados por la afección a los procesos de negocio de la política de seguridad diseñada. En estos costes, que usualmente son subjetivos, deberán valorarse los costes derivados de la dificultad de uso para los usuarios que conlleva cumplir la disciplina de seguridad derivada de la política, las restricciones de servicios y funcionalidades provocadas por la política de seguridad y la reducción de prestaciones que se puede dar en los servicios, derivadas de las tecnologías de seguridad.

El coste total de la seguridad será la suma de dos componentes:

- Costes (directos más indirectos) provocados por la introducción de medidas de seguridad.

- Costes provocados por los impactos de los riesgos no cubiertos por la política de seguridad.

Se puede analizar la evolución de estos costes en función del tanto por ciento de riesgos afrontados por la política de seguridad; los costes de implantación son costes que aumentarán a medida que se decide afrontar más riesgos de la tabla de riesgos, y este aumento no es lineal, sino que usualmente conlleva un crecimiento exponencial, de forma que la utopía de la seguridad absoluta (100% de riesgos cubiertos) tendría un coste infinito. Por otra parte, el coste provocado por los impactos de los riesgos no cubiertos decrecerá a medida que se afrontan más riesgos por la política de seguridad. Este decrecimiento puede considerarse más o menos lineal, llegando a impactos teóricamente nulos si el 100% de los riesgos estuvieran cubiertos por la política de seguridad.

Esto hace que el coste total de la seguridad, expresado como la suma de ambos componentes tenga un cierto mínimo, tal y como se muestra en la Figura 2:

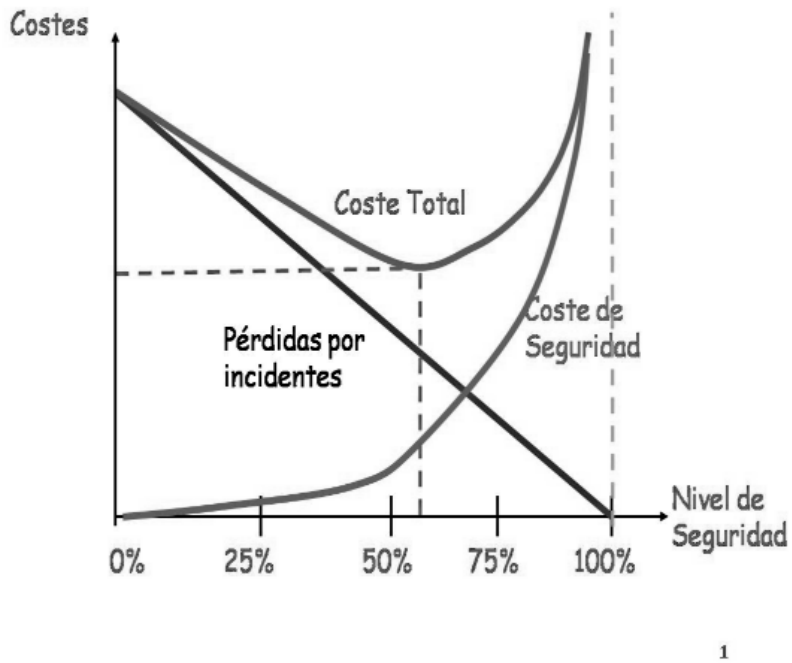

Figura 2: Punto de equilibrio financiero

Este mínimo representa el tanto por ciento de riesgos óptimo que debe cubrir la política de seguridad. Cubrir menos riesgos implica que existen riesgos cuyo impacto económico es mayor que el coste de las medidas para evitar dicho riesgo; cubrir más riesgos implica que se está gastando más dinero en evitar un riesgo que el dinero que se puede perder por el impacto del mismo.

La identificación de este punto de equilibrio financiero de la seguridad desvela los riesgos que deben ser afrontados por la política de seguridad. A partir de aquí, es necesario diseñar una política de seguridad que permita disminuir la importancia de esos riesgos mediante dos tipos de actuación:

- Medidas defensivas, que disminuyan la vulnerabilidad de la organización asociada a ese riesgo y por tanto, disminuyan la importancia del riesgo.

- Medidas de seguro, que disminuyan el impacto del riesgo y por lo tanto, su importancia.

La política de seguridad debe ser diseñada como un conjunto de procedimientos y actuaciones destinado a disminuir la importancia de estos riesgos. Estos procedimientos y actuaciones imponen una disciplina que puede ser implantada mediante productos y tecnología de seguridad, o simplemente recomendados, en cuyo caso se habla de pautas de uso apropiado. Es importante que la política de seguridad se publicite y difunda adecuadamente entre los usuarios de la organización, de forma que se sepa claramente y en todo momento cuáles son las vías correctas de utilización de los servicios y sistemas de información de la organización [6].

Capítulo 2

Las amenazas de Internet

2. Las amenazas de Internet

Antes de explicar los servicios de seguridad que la tecnología actual proporciona para la protección de entornos de sistemas de información interconectados, en este capítulo se detalla uno de los componentes del ciclo de seguridad vistos anteriormente: las amenazas de personal externo malintencionado que, a través de la conexión a Internet de una organización, intenta realizar ataques contra sus sistemas de información. Estas amenazas constituyen la mayor diferencia del análisis de seguridad de los sistemas interconectados respecto al análisis de seguridad en otro tipo de ámbitos, por lo que es conveniente realizar un estudio más completo de este tipo de ataques.

2.1 El atacante de Internet

El aumento de la utilización de los servicios que se ofrecen sobre Internet ha evolucionado en paralelo a la identificación de múltiples problemas asociados a la falta de seguridad con la que se diseñaron y/o desarrollaron muchos de estos servicios y protocolos de Internet.

Cuando los principales protocolos y servicios de Internet fueron diseñados (en las décadas de 1970 y 1980 principalmente), no se pensaba en una utilización tan global como la que se da en la época actual, sino en una utilización orientada a organismos de investigación y académicos, que constituían un entorno más o menos de confianza en el que la seguridad no era uno de los aspectos clave a considerar en el diseño de los protocolos y servicios. Por ese motivo, muchos de los protocolos que se utilizan actualmente cuentan con graves problemas de seguridad: protocolos que envían las claves de acceso en claro (POP, TELNET, etc.), protocolos que no requieren una autenticación entre las partes (SMTP), etc.

Por otra parte, en el desarrollo de las aplicaciones que permiten proporcionar los servicios de Internet, durante bastante tiempo tampoco se tuvieron en cuenta las pruebas exhaustivas de seguridad, ya que nuevamente se partía de una base implícita, la utilización en un entorno de confianza, por lo que se consideraba más importante el desarrollo correcto de la funcionalidad de los servicios, que su tolerancia a situaciones anómalas que en situación normal no debían de suceder.

Estos factores, unidos a la expansión del uso de estos servicios más allá de los ámbitos investigador y científico, han dado lugar a la identificación de múltiples fallos de seguridad explotables en la implementación de servicios de Internet. Sin embargo, descubrir estos fallos no es tarea fácil en

la mayoría de las ocasiones, sino que está sólo al alcance de verdaderos expertos que controlan diversas disciplinas relacionadas (sistemas operativos, lenguajes de programación de bajo nivel, protocolos de red, etc.), y que hacen posible que el universo de probables atacantes sea teóricamente reducido y potencialmente controlable. El problema surge cuando estos "expertos" deciden en un momento dado publicitar sus descubrimientos en Internet, muchas veces incluso sin informar a las compañías de software cuyos productos son, de repente, vulnerables, llegando en ocasiones a proporcionar métodos fáciles de utilizar ("pruebas de concepto con fines educativos", según su terminología), que cualquiera puede descargarse y explotar la vulnerabilidad descubierta.

Aquí surge el verdadero problema de las amenazas de Internet: se pone a disposición de todo el mundo las armas con las que se puede atacar a los sistemas informáticos. No es necesario un gran nivel técnico para poderlas utilizar, por lo que diversos sectores que no tienen una madurez suficiente en la utilización correcta de las tecnologías pueden utilizarlas indiscriminadamente sin tener una consciencia de las posibles consecuencias. En este entorno surgen distintos perfiles de "atacantes de Internet":

- El perfil del atacante que busca un beneficio económico derivado de su ataque. Esta es la causa más común de los delitos en el campo de la delincuencia tradicional. Sin embargo, en el área de la seguridad en redes de telecomunicación es el perfil minoritario. Ejemplos de estos ataques son los ataques a entidades bancarias para realizar transferencias de fondos, el espionaje industrial, etc.

- El perfil del vándalo: el atacante que no busca ningún beneficio económico pero que causa destrozos y daños en la máquina atacada deliberadamente. Este perfil también existe en la delincuencia tradicional pero es bastante menos numeroso que el anterior (por ejemplo, el vándalo que destroza mobiliario urbano, etc.).

- El perfil del "juguetón": este perfil es el más peculiar de todos, ya que es específico del ámbito de Internet, sin tener normalmente equivalente en la delincuencia tradicional. Se trata del atacante que realiza ataques sólo para demostrarse que es capaz de hacerlo, o creyendo que está haciendo un favor al propietario del sistema atacado. Una vez ejecutado el ataque (normalmente entrar sin autorización en algún sistema), no van más allá, por lo que no suelen ser conscientes de que están realizando un ataque potencialmente dañino, sino que para ellos se trata de un reto tecnológico, considerándolo incluso como un favor al atacado, al haber descubierto una vulnerabilidad en sus sistemas que le notifican posteriormente.

Sin embargo, este tipo de actividades lejos de suponer un beneficio para el atacado, supone un grave problema, ya que un buen operador de sistemas ante cualquier indicio de ataque de seguridad no debería simplemente corregir la vulnerabilidad y continuar, sino que como se desconoce el alcance verdadero del ataque (el atacante podría haber modificado información, o introducido programas falsos, etc.), ese sistema pasa a ser no confiable y suele exigir, en la mayoría de los casos, una reinstalación con los perjuicios que ello conlleva de disponibilidad de servicios y tiempo invertido por los operadores.

Ante este panorama, resulta interesante ver otros factores, aparte del supuesto reto tecnológico, que han propiciado la aparición y progresión de los atacantes de Internet, sobre todo del perfil del "juguetón":

- No existe un entorno hostil a la realización del ataque. Mientras que en la delincuencia clásica si alguien te descubre realizando el acto delictivo puede actuar en tu contra (llamando a la policía, gritando, etc.), en los ataques de Internet no existen normalmente posibles observadores del ataque, se puede hacer a cualquier hora y desde cualquier sitio.

- Durante algún tiempo, el tratamiento que se dio a estos incidentes desde los medios de comunicación fue equivocado. La novedad de estos ataques y su componente tecnológico hacían que muchas veces fueran destacados con una importancia que no merecían, produciendo un efecto perverso: se propiciaba indirectamente la aparición de nuevos atacantes que veían que sus acciones podían tener una gran repercusión.

- Hubo una etapa de transición en la que no existía una legislación adecuada, por lo que estas acciones se movían en una especie de "limbo legislativo", que hacía que no pudieran ser perseguidas adecuadamente. Actualmente la mayoría de los países ya tienen una legislación adecuada que incluye, de una manera u otra, las actuaciones que se pueden denominar ataques de Internet.

Por todo lo anterior, resulta necesaria una concienciación sobre el problema de la seguridad en Internet, no sólo desde un punto de vista técnico, sino también social, ya que igual que técnicamente es sencillo realizar muchos ataques de delincuencia clásica, en Internet también pueden realizarse. Por ello, se debe educar a la sociedad para romper la visión de "reto tecnológico" que se tiene muchas veces en estas situaciones, inculcando la idea del daño que se causa con estos ataques.

2.2 Vulnerabilidades de la conexión a Internet

Se ha visto anteriormente que muchos de los problemas de seguridad en Internet se deben a los fallos de seguridad cometidos en el diseño de los protocolos y servicios de Internet, y en el desarrollo de las aplicaciones que los implementan. El ataque más efectivo es aquel que permite ser realizado sobre sistemas ajenos, de los que no se tiene más conocimiento que su existencia. Pero ¿cómo se puede acceder a un sistema ajeno, del que no se conoce nada? La respuesta es simple, igual que en la seguridad tradicional del hogar:

- Si se ha robado, falsificado o duplicado una llave, se entrará por la puerta sin "romper" nada.

- Si no se tiene ninguna llave, se tendrá que "romper" o forzar algún punto de acceso a la vivienda.

En los sistemas informáticos ocurre algo similar: si se ha adivinado o robado una clave, se accederá al sistema como un usuario normal, sin tener que "romper" nada. Si no se posee esta clave, se tendrá que "romper" algún punto de acceso al sistema. Los puntos de acceso a un sistema son aquellos puntos que permiten poder enviarles algo remotamente en cualquier momento, que posteriormente tratan de procesar. Son los denominados servidores de Internet, aplicaciones que están escuchando continuamente en la red por si llega alguna petición hacia ellos que tienen que responder. Existen muchos ejemplos de servidores de Internet, desde servidores muy especializados como servidores de acceso a bases de datos o aplicaciones especializadas, hasta servidores muy comunes como un servidor Web o de correo electrónico, o incluso servidores de acceso compartido a disco, muy común en la mayoría de los ordenadores de usuario.

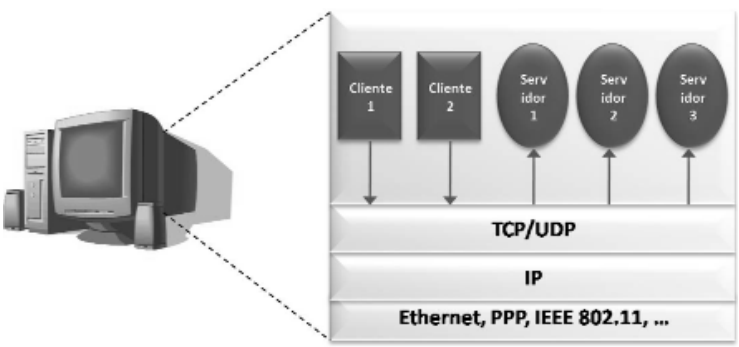

Figura 3: Servidores de red

En la Figura 3 se puede ver la torre de comunicaciones de un sistema, en la que por encima de las torres de protocolos (subred, red y transporte), se encuentra el nivel de aplicación donde se pueden tener aplicaciones clientes (representadas con un rectángulo) y aplicaciones servidoras (representadas con un óvalo). Las aplicaciones clientes están orientadas para su utilización por un usuario, por lo que no escuchan en la red, sino que lanzan peticiones originadas por el usuario y esperan las respuestas a dichas peticiones. Por el contrario, las aplicaciones servidoras están orientadas a dar servicio a clientes remotos, por lo que deben estar escuchando continuamente para recoger los datos que el nivel de transporte le puede entregar en cualquier momento. Por ello, resulta mucho más fácil atacar a este último tipo de aplicaciones en Internet, ya que están siempre a la escucha de posibles peticiones, lo cual permitirá enviarle datos en cualquier momento. Si estos datos están construidos de forma anormal y maliciosa y la aplicación no está desarrollada para responder adecuadamente a esas anormalidades, se puede dar el principal ataque de Internet, el acceso remoto a un sistema.

Antes de describir en detalle los posibles ataques que se pueden dar en Internet, es conveniente categorizarlos:

- Ataques por ser alcanzables desde Internet. En estos ataques no es necesario que la máquina esté siendo utilizada por un usuario, sino que basta con que el sistema esté conectado a Internet y pueda recibir paquetes de datos a través de Internet que intentará procesar (que sea alcanzable desde Internet) [7]. Se distinguen dos tipos de ataques de este tipo:

  - Acceso remoto no autorizado. Mediante el envío de datos maliciosos se consigue acceder a los recursos de la máquina como usuario remoto, acceder al disco del sistema, etc.

  - Negación de servicio. Mediante el envío de datos maliciosos se consigue que el sistema completo o alguno de los servicios que alberga, tenga un fallo que lo convierta en inaccesible.

- Ataques por la actividad de un usuario en Internet. Si el sistema es utilizado por un usuario que usa servicios de Internet con aplicaciones cliente, el sistema y/o usuario es vulnerable a otro tipo de ataques:

  - Desprotección de la intimidad. Toda la actividad del usuario en Internet puede ser registrada, y utilizada posteriormente.

- Vulnerabilidades de las aplicaciones clientes, que pueden provocar un acceso remoto no autorizado o una negación de servicio.

- Ataques de ingeniería social, cuyo fin es engañar al usuario para que éste realice acciones que permitan realizar un ataque, bien directamente (virus), o indirectamente abriendo una vía de acceso para un atacante posterior (caballo de troya).

- Acceso a la información en tránsito del usuario, cuando viaja por la red.

En las siguientes secciones se proporcionan detalles sobre estos ataques.

2.2.1 Ataques por ser alcanzable desde Internet

2.2.1.1 Acceso remoto no autorizado

Este ataque es el ataque más efectivo de Internet, ya que permite al atacante acceder a todos los recursos del sistema atacado pudiéndose hacer con su control total. Existen diversas formas de realizar un ataque de este tipo:

- Aprovechar una vulnerabilidad en el software de los servidores de red.

- Aprovechar una vulnerabilidad en la configuración de los servidores de red.

- Aprovechar una vulnerabilidad en la implementación de la torre de protocolos.

Vulnerabilidad en el software de los servidores de red

Como se ha dicho anteriormente, los servidores de red son aplicaciones que se ejecutan en el sistema y que están escuchando en el nivel de transporte para recoger los datos que le envían e intentar procesarlos. Estas aplicaciones son programas desarrollados por programadores, que pueden incluir errores de programación no detectables en un entorno de funcionamiento normal. Si estos errores de programación se manifiestan como consecuencia de la llegada de datos maliciosos a través de la red, el servidor va a intentar ejecutar las instrucciones que ha recibido, provocando que el atacante pueda coger el control del sistema al lograr que éste ejecute las órdenes que envía por la red.

El caso más frecuente de este tipo de errores es el denominado "desbordamiento de *buffer*" o "*buffer overflow*", ilustrado en la Figura 4.

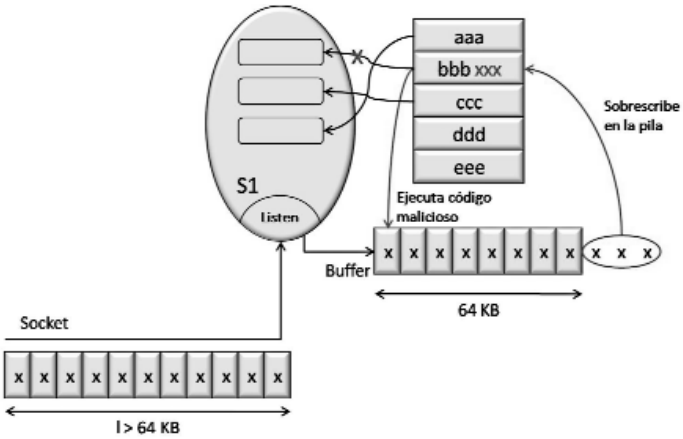

Figura 4: *Buffer overflow*

Los pasos que rigen el comportamiento habitual de este ataque son los siguientes:

1. El servidor reserva unas posiciones de memoria para almacenar los datos que le llegan por la red. Para estimar el tamaño de la memoria a reservar, el programador comprueba cuál es el tamaño máximo de los datos que le pueden llegar según el estándar del protocolo implementado. En principio, se supone que no deberían llegar datos de tamaño superior al máximo permitido por el estándar.

2. Un atacante genera un paquete de datos malicioso con un tamaño superior al máximo permitido.

3. El servidor recibirá esos datos y los irá almacenando en la memoria reservada. Cuando el servidor llena el espacio reservado se pueden dar dos situaciones:

   a) El servidor comprueba la situación y advierte que el tamaño de los datos enviados supera el máximo permitido, por lo que rechaza la petición por no ser conforme al estándar. En este caso, no se da opción a la realización de un ataque.

b) El servidor no comprueba la situación y sigue transfiriendo los datos a memoria, sin darse cuenta de que los está enviando a posiciones de memoria que no han sido reservadas y que, por lo tanto, está sobrescribiendo posiciones de memoria. Es en este caso, cuando se puede intentar realizar el ataque.

4. Si el servidor no comprueba el desbordamiento de *buffer*, el comportamiento más normal es intentar sobrescribir posiciones de memoria protegidas por el sistema operativo, caso en que el propio sistema operativo aborta la ejecución del servidor con un mensaje de error. No obstante, existe un caso en el que se sobrescriben posiciones de memoria especiales, las correspondientes a la pila del sistema operativo, que contienen las direcciones de las instrucciones que el sistema operativo va a ejecutar.

5. Si el atacante consigue que uno de los datos que se desborda del *buffer* sobrescriba la pila del sistema operativo, puede forzar la escritura de la dirección del *buffer* de memoria donde el servidor ha ido almacenando los datos que le ha enviado previamente el atacante.

6. Por último, el sistema operativo intentará ejecutar el código apuntado desde la pila, es decir, intentará ejecutar el contenido de los datos que el atacante ha enviado previamente. Si estos datos contienen instrucciones que permiten al atacante hacerse con el control del sistema, el sistema operativo lo ejecutará y el atacante habrá realizado con éxito un acceso remoto no autorizado al sistema.

Este tipo de vulnerabilidad es la más frecuente en los servidores de red, y por tanto, la más explotada actualmente. No obstante, existen otras vulnerabilidades del software de los servidores de red menos frecuentes, que también pueden ser explotadas, como son el paso de parámetros inadecuados, condiciones de carrera entre procesos, etc.

Ante este tipo de ataques, la mejor estrategia de defensa es mantener constantemente actualizados los servidores de red. Un servidor desactualizado es una bomba de relojería instalada en un entorno, que con gran probabilidad será descubierta y explotada. Los fabricantes de estos servidores sacan frecuentemente parches de seguridad que deben ser instalados lo antes posible por los usuarios. Por supuesto, un entorno no debe incluir servidores que no se utilizan (durante mucho tiempo la instalación por defecto de conocidos sistemas operativos incluía la instalación de servidores de red, independientemente de que fueran a usarse o no).

Existen también nuevas estrategias de defensa para evitar técnicamente estos comportamientos de ejecución de código malicioso debido a desbordamientos de *buffer* y errores inesperados. Es lo que se denomina "*Data Execution Prevention* (DEP), incluido por Microsoft en las últimas versiones de sus sistemas operativos, que se basa en marcar las zonas de memoria que contienen código ejecutable, e impedir que se ejecuten instrucciones en zonas de memoria no marcadas al efecto. Esta protección puede realizarse vía hardware (para ello, el microprocesador debe soportarlo) o software.

Vulnerabilidades en las configuraciones de los servidores de red

Otra potencial fuente de vulnerabilidades es la configuración que se realiza de los servidores de red. Aunque el programa servidor no incluya vulnerabilidades debidas a errores de programación, este servidor deberá ser configurado adecuadamente por el administrador del sistema, configuración que puede estar sujeta a errores que pueden potencialmente abrir agujeros de seguridad que permitan un acceso remoto no autorizado.

El mayor problema surge cuando la configuración por defecto del servidor de red es insegura. En múltiples ocasiones, las configuraciones de los servidores instalados en los sistemas son aquellas que vienen por defecto, o pequeñas variaciones de ellas, por lo que si la configuración por defecto es insegura, esta vulnerabilidad se transmitirá a múltiples instalaciones. Actualmente es muy poco frecuente encontrar este tipo de vulnerabilidades, pero se han dado ejemplos famosos, como servidores del servicio NFS (*Network File System*), que con la instalación por defecto se permitía a cualquier persona acceder (sólo en modo lectura) a los datos de los discos duros, o el servicio de X-Windows (entorno gráfico utilizado en sistemas tipo UNIX), en el que por defecto cualquiera podía solicitar el contenido de la pantalla de otro usuario en un instante concreto.

La defensa ante estas malas configuraciones pasa por detectarlas y corregirlas, para lo que existen múltiples programas, los denominados sistemas de auditoría de seguridad, que hacen un análisis de seguridad del sistema y notifican de las potenciales vulnerabilidades que presentan.

Vulnerabilidades en la implementación de la torre de protocolos

La última vía para poder acceder a un sistema remoto que no tiene vulnerabilidades en el software de los servidores, ni configuraciones deficientes de éstos, consiste en intentar encontrar un fallo en la torre de protocolos utilizados para acceder al servicio. Normalmente, esto se traduce en encontrar un fallo de seguridad en la implementación de los niveles de subred, red (IP) y transporte (TCP o UDP) [8].

Se trata de las vulnerabilidades menos frecuentes, pero también de las más peligrosas, dado que afectan normalmente a nivel de sistema operativo, convirtiendo en vulnerables todos aquellos sistemas que tengan dicho sistema operativo instalado.

Una de las vulnerabilidades más famosas fue el ataque denominado "ataque del día de Navidad", realizado el 25 de Diciembre de 1995, en el que se combinaba la falsificación de la dirección IP origen con una deficiente generación de números aleatorios en los paquetes de sincronismo del protocolo TCP, que permitía que un atacante explotara una relación de confianza entre dos sistemas, suplantando a uno de ellos ante el otro en una sesión TCP [9].

2.2.1.2 Ataques de negación de servicio

Un ataque a un sistema remoto, menos refinado que los anteriores, es provocar el fallo del sistema remoto o de alguno de los servicios que se ejecutan en él.

Una de las formas más frecuentes de conseguir estos ataques es explotar una vulnerabilidad del software de los servidores de red, como las de desbordamiento de *buffer* vistas anteriormente, pero en este caso no es necesario sobrescribir la pila del sistema, sino que es suficiente con que se desborde a posiciones de memoria protegidas por el sistema operativo, ya que éste se encargará de cerrar la aplicación que falla con lo que se consigue el efecto de negación de servicio perseguido.

Existen ejemplos muy famosos de ataques de negación de servicio, como el "*ping* de la muerte", consistente en enviar un paquete del protocolo ICMP con una mochila de datos (*payload*) mayor de 64 KB, lo cual excede el tamaño máximo permitido en el protocolo. En ciertas versiones de sistemas operativos, la recepción de estos mensajes maliciosos provocaba la caída total del sistema. Además, el envío de estos mensajes era muy sencillo, simplemente había que utilizar el conocido programa "*ping*" con los parámetros adecuados. Este tipo de ataque no tiene efecto sobre los sistemas operativos actuales.

Una variante de estos ataques de negación de servicio es el bombardeo, o *bombing*. Consiste en inundar de peticiones a un cierto sistema con el fin de que no pueda procesar todas las peticiones y se produzca un fallo o quede inoperativo. Un ejemplo de este tipo de ataques son los ataques de negación de servicio distribuidos (DDoS - *Distributed Denial of Service*), consistentes en sincronizar cientos o miles de procesos para que

en un determinado instante, todos comiencen a realizar peticiones masivamente a un servidor, peticiones diseñadas, además, sabiendo que exigen un cierto esfuerzo de procesamiento por el servidor. Ante esta avalancha de peticiones, los servidores pueden quedar inutilizables para proporcionar cualquier otro tipo de servicio legítimo. Un ejemplo de este tipo de ataque es lo que se conoce como el *Mail Bombing*, que consiste en tratar de atacar un servidor mandando una avalancha de mensajes de correo electrónico de gran tamaño, pudiendo dejar inoperativo la recepción de correos legítimos durante grandes periodos de tiempo.

2.2.2 Ataques provocados por la actividad de un usuario

En los párrafos anteriores, se han analizado las vulnerabilidades que tiene un sistema por el hecho de ser alcanzable desde Internet. Los ataques definidos ocurren por la explotación de vulnerabilidades de algunos de los componentes de la pila de comunicaciones del sistema, desde la aplicación servidora o su configuración, hasta la implementación de la torre de protocolos. Pero en ningún momento se tiene en cuenta el punto más débil de un sistema informático, el usuario. Si un sistema, además de albergar servicios que pueden ser atacados, tiene aplicaciones de tipo cliente que son ejecutadas por un usuario, existen nuevas e importantes vulnerabilidades derivadas de este hecho. En esta sección se describen las más importantes.

2.2.2.1 Desprotección de la intimidad

La utilización de servicios de Internet por parte de un usuario puede estar generando ciertas vulnerabilidades derivadas de la recolección de datos por parte de un tercero de la actividad de dicho usuario [10]. En efecto, la navegación por páginas Web va dejando muchos rastros del usuario en el servidor, como la dirección IP del usuario, la página desde la que procede, el tipo de navegador que usa, el sistema operativo que utiliza, versión de Java instalada por el usuario, las fuentes cargadas, etc. Incluso versiones anteriores de navegadores, cuando navegaban por ciertas páginas maliciosas podían provocar el envío inadvertido de un correo electrónico desde la máquina del usuario, que desvelaba la dirección de correo electrónico del usuario.

Aparte de la navegación por páginas Web, hay otros servicios cuya utilización puede ser explotada para recabar información personal, como por ejemplo, mensajes enviados a foros de discusión, en los que se puede haber publicado la dirección de correo electrónico, páginas personales de Web en las que se publican datos de contacto, incluyendo el correo electrónico, etc.

Caso aparte son los programas espías, que pueden ser instalados en el sistema del usuario utilizando técnicas de ingeniería social, como se verá más adelante. Estos programas están diseñados para recabar información sobre el usuario y su actividad, y enviárselo a determinados destinatarios que podrán utilizarla sin tener permiso para ello. La utilización de toda esta información recolectada sobre los usuarios puede ser muy variada:

- El mero hecho de tener información sobre un usuario delata su existencia y la del sistema que utiliza, pudiendo ser incluido como objetivo de potenciales ataques. El sistema más seguro es el que nadie sabe que existe.

- La captura de la dirección de correo electrónico del usuario hace que esta dirección pueda ser incluida en listas de envío de correo no solicitado o spam.

- Aunque quizás, la utilización más refinada de toda esta información es el denominado marketing personalizado. Un procesado de la actividad de un usuario en Internet puede desvelar mucha información acerca del perfil personal de dicho usuario, como los sitios que suele visitar, qué días y a qué horas los visita, etc. Un adecuado procesado de toda la información sobre los hábitos de navegación Web de un usuario mediante técnica de extracción de significado de grandes volúmenes de información, como las técnica de minería de datos, pueden permitir generar un perfil sobre los gustos y aficiones del usuario bastante acertado. Estos perfiles tienen una gran utilización por parte de las técnicas de marketing, como por ejemplo la generación de publicidad a la medida del usuario cuando éste se conecta a un sitio Web. La siguiente vez que el usuario se conecta a un sitio Web, la publicidad mostrada ya no es publicidad genérica, sino que es publicidad generada exclusivamente para él, en función de sus gustos y aficiones tomados de su perfil personal. El índice de impacto de este tipo de publicidad personalizada es muchísimo mayor que la publicidad genérica, suponiendo un potencial negocio muy importante.

2.2.2.2 Vulnerabilidad en aplicaciones cliente

Al igual que las aplicaciones servidoras de red pueden tener fallos de programación que permiten generar vulnerabilidades de seguridad, las aplicaciones que se usan como clientes de Internet también están sujetas a estos fallos de programación y por lo tanto, a potenciales vulnerabilidades de seguridad. La diferencia esencial es la ventana de vulnerabilidad, es decir, mientras que en las aplicaciones servidoras se puede realizar el ataque en cualquier momento, ya que estas aplicaciones están siempre ejecutándose y escuchando en la red para recoger peticiones, las aplicaciones cliente no escuchan en la red, sino que mandan peticiones guiadas por la actividad de un usuario, y esperan a recibir las respuestas a estas peticiones desde el servidor. Por lo tanto, la única ventana de vulnerabilidad posible reside en las respuestas a las peticiones generadas por los clientes. Si el atacante es capaz de introducirse en un servidor, podrá manipular las respuestas que éste genera a los usuarios. Por ejemplo, si un atacante tiene consciencia de que una aplicación cliente de navegación por la Web (un navegador Web) está sujeta a alguna vulnerabilidad, el atacante podrá intentar atacar servidores Web para, por ejemplo, alterar las páginas HTML de manera que incluyan anomalías maliciosas destinadas a explotar las vulnerabilidades del navegador Web cuando intente procesar dicha página HTML.

La dificultad del ataque reside en ser capaz de introducirse en las respuestas recibidas por el usuario. Para ello, el atacante debe ser capaz de alterar los contenidos de algún servidor que sepa que el usuario vulnerable utiliza, o bien intentar engañar al usuario para que se conecte a un servidor específico controlado por el atacante y que contenga contenidos maliciosos.

Las vulnerabilidades más frecuentes de las aplicaciones cliente se dan en los navegadores de Internet, cuando reciben páginas HTML con contenido malicioso cuyo objetivo es explotar un posible fallo de programación a la hora de procesarlas. Este fallo además, puede ser extensible a otras aplicaciones que hacen uso de las librerías de procesado HTML de los navegadores Web. Por ejemplo, muchos clientes de correo electrónico recurren a la funcionalidad de los navegadores para mostrar un mensaje de correo electrónico recibido en formato HTML. De esta manera, la simple visualización de un mensaje de correo electrónico podría estar explotando un fallo de programación que permitiera un ataque de seguridad al sistema.

Otra fuente muy importante de vulnerabilidades de seguridad en aplicaciones cliente es el hecho de que en las páginas HTML puede transmitirse código ejecutable, como por ejemplo Java, Javascript o ActiveX. Los navegadores tienen grandes precauciones a la hora de ejecutar estos códigos,

pero aun así han existido graves vulnerabilidades de seguridad provocadas por fallos en los navegadores a la hora de restringir la ejecución de dichos comandos.

2.2.2.3 Ataques de ingeniería social

Todos los ataques vistos hasta ahora se basan en la explotación de las vulnerabilidades de seguridad de los sistemas, mediante la utilización de distintas técnicas. Sin embargo, el punto más débil de un sistema no son las aplicaciones ni los protocolos, sino el usuario que los utiliza. Por ello, existen múltiples ataques orientados a "explotar vulnerabilidades" del usuario final, conocidos como ataques de ingeniería social, que intentan aprovechar la falta de conocimientos técnicos de un usuario medio sobre sistemas informáticos.

Básicamente, los objetivos de estos ataques son:

- Conseguir que el usuario ejecute un determinado programa.

- Conseguir que el usuario proporcione información confidencial (claves de acceso, información privada, etc.).

Existen múltiples métodos para intentar engañar al usuario:

- Ataques de *phishing*, cuyo fin es conseguir información confidencial. Mediante mensajes de correo electrónico intentan dirigir al usuario a servidores Web que falsifican la apariencia de un servidor Web verdadero, para que el usuario introduzca sus claves de acceso.

- Mediante correo electrónico, enviando mensajes al usuario para que ejecute un cierto programa. Estos ataques han evolucionado con el fin de tratar de evitar las sospechas de los usuarios, como por ejemplo, enviar los programas camuflados con dobles sufijos para que el usuario no los identifique en principio como programas ejecutables, enviarlos falsificando el remitente para que parezca el administrador de tu dominio, etc.

- Propagándose desde equipos infectados a equipos o destinatarios cercanos. Una vez que un usuario ha sido engañado y ha ejecutado algún programa, este programa puede intentar utilizar el sistema del usuario para tratar de engañar a los usuarios cercanos o conocidos de éste. Por ejemplo, puede enviar mensajes de correo electrónico a la lista de direcciones del usuario infectado utilizando su propio remite, lo cual dotará a estos mensajes de una cierta confianza al provenir de una persona conocida, o utilizar otros mecanismos como la mensajería instantánea y los contactos del usuario.

Este tipo de ataques de ingeniería social cuyo objetivo es conseguir que el usuario ejecute un cierto programa malicioso, eran los antiguamente denominados virus. Pero hoy en día, este término se ha quedado corto para abarcar a todos los posibles tipos de programas maliciosos que pueden ser ejecutados con engaño, y hoy se engloban bajo el término genérico "*malware*" todos los posibles programas maliciosos [11]:

- Virus: programas destinados a realizar un ataque de negación de servicio en el equipo infectado, con la posibilidad de propagarse a otros equipos.

- Caballos de Troya: programas que ejecutan un servidor de Internet en el equipo infectado que permiten un acceso remoto posterior al atacante.

- Programas espía o *Spyware*: programas que monitorizan el uso de aplicaciones o de la información almacenada en el disco, y la envían posteriormente a un atacante para que éste la pueda utilizar.

- Programas distribuidores de correo basura: programas que convierten al ordenador del usuario en remitente involuntario de correo basura masivo.

- Programas pasarela de ataques: programas que permiten que el sistema infectado realice un cierto ataque a otros programas, como por ejemplo un ataque de negación de servicio distribuido (DDoS). Estos, normalmente, son las denominadas redes de software robot o *botnet*.

La defensa ante estos ataques debe realizarse en dos facetas distintas:

- Una faceta educativa, en la que es necesario educar a los usuarios y hacer campañas de concienciación que eviten los engaños al usuario, instándoles a no ejecutar nunca programas recibidos por correo electrónico, ni proporcionar contraseñas según las instrucciones recibidas en un correo electrónico, etc.

- Una faceta técnica, tratando de detectar la ejecución de estos programas maliciosos y frenándoles antes de que ejecuten su código malicioso. Éste es el objetivo tradicional de los programas antivirus que han tenido que evolucionar para incluir la detección de programas espía, caballos de Troya, etc.

2.2.2.4 Correo electrónico no deseado

Aunque no puede catalogarse como un ataque, el problema del correo electrónico no deseado, más conocido como SPAM, es un grave problema actualmente debido a su magnitud. Si bien no es intrínsecamente malicioso, el impacto de este problema es más grave actualmente que muchos de los ataques maliciosos que se dan en Internet.

El funcionamiento es simple: una empresa consigue millones de direcciones de correo electrónico y se dedica a enviar a todas esas direcciones publicidad no solicitada. Si una pequeñísima fracción de receptores hace caso de la publicidad, el negocio está hecho. Para ello se necesita:

- Obtener grandes listas de direcciones de correo electrónico.

- Realizar el envío masivo de correos electrónicos sorteando las contramedidas que se realizan contra el SPAM.

Por lo tanto, la primera medida necesaria para evitar la recepción de correo basura, es la protección de la dirección de correo electrónico. Esta protección implica que no esté publicada en ningún sitio accesible desde Internet, tal como páginas Web, foros, etc. Sin embargo, este hecho puede acarrear algunos inconvenientes, como por ejemplo que nadie sepa como contactar con el resto de personas legítimamente por correo electrónico. Por ello, y dado que normalmente los rastreadores de direcciones de correo electrónico son programas y no seres humanos operando manualmente, se pueden tomar algún tipo de medidas alternativas:

- Publicar la dirección de correo electrónico en páginas Web como imagen, en vez de como texto. De esta manera, los robots que rastrean texto buscando direcciones de correo electrónico no podrán encontrarla y una persona que lo vea sí podrá interpretarla. Sin embargo, los robots ya conocen esta técnica y existen robots que son capaces de procesar las imágenes buscando direcciones de correo electrónico. En ese caso, es necesario recurrir a las deformaciones de los caracteres para que el programa de procesado no los pueda reconocer, manteniendo la legibilidad para los usuarios que ven dichas imágenes. A este tipo de técnica se le conoce como "*captcha*" y es cada vez más utilizada en Internet para evitar el procesado automático de formularios por robots.

- Modificar la dirección de correo electrónico de manera que un robot recoja la dirección modificada, pero una persona sea capaz de reconocer perfectamente que está modificada y generar la dirección ori-

ginal. Por ejemplo, un usuario podrá publicar su dirección de correo electrónico como nombre.apellido@miempresa-quitaesto.com; de esta manera se asegura que los robots no podrán automáticamente saber su dirección de correo electrónico, pero un usuario sí.

En caso de que una dirección de correo electrónico haya sido capturada para el envío de correo basura, las medidas más efectivas pasan por:

- Identificar el correo y filtrarlo para que no se mezcle con el correo legítimo.

- Identificar el causante y denunciarle a su proveedor de Internet.

Los programas que permiten identificar el correo basura han evolucionado mucho los últimos años y ya poseen una efectividad muy grande, disminuyendo en gran medida el número de falso positivos (mensajes legítimos identificados como correo basura) y falso negativos (correo basura no identificado). Estos filtros se pueden poner directamente en el ordenador del usuario, de manera que el usuario recoge todo el correo de su buzón y realiza el filtrado localmente en su ordenador, o en el servidor de correo, de forma que el propio servidor realiza el filtrado y sólo entrega correo legítimo en el buzón de los usuarios (o entrega todo, pero etiquetando el correo identificado como basura).

Otra medida que evita la recepción de correo basura, ya nombrada en líneas anteriores del texto, es la identificación del originador del correo para poder denunciarlo ante su proveedor de Internet. Es evidente que un originador de correo basura no va a utilizar su dirección de correo real ya que se le podría identificar fácilmente y denunciar, sino que se aprovecha de una debilidad de seguridad del correo electrónico que permite de forma sencilla falsificar el remitente de un mensaje de correo electrónico. Sin embargo, un examen detallado de las cabeceras de un correo electrónico recibido puede dar mucha información acerca del verdadero originador de un correo electrónico basura, o al menos de su proveedor de Internet.

Cuando un mensaje es enviado, se utiliza el protocolo SMTP para su transmisión desde el ordenador del usuario remitente hasta el servidor de correo electrónico de su proveedor de Internet, el cual buscará el servidor del destinatario y se lo enviará también utilizando el protocolo SMTP, como se describe en la Figura 5. Para la entrega del correo desde el servidor del destinatario al usuario final, se utiliza POP o IMAP, como se muestra en la figura.

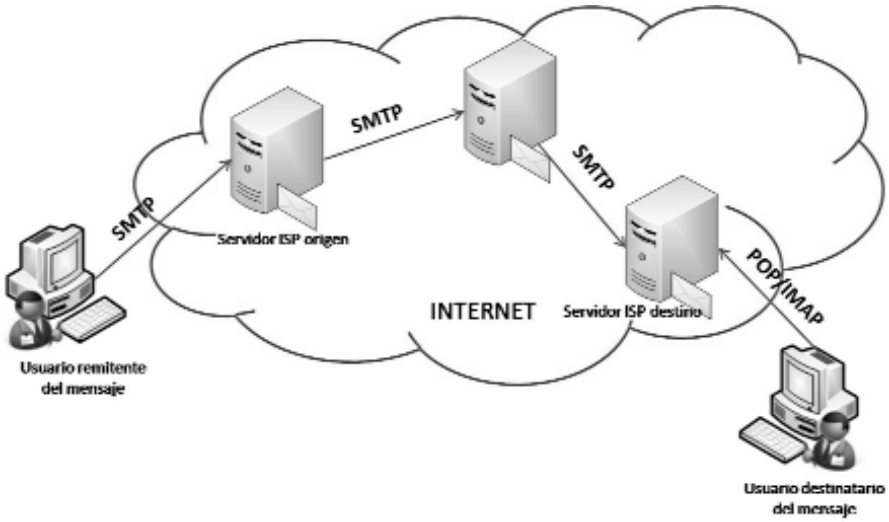

Figura 5: Envío de mail con SMTP

Las recepciones del mensaje mediante el protocolo SMTP en cada nodo intermedio que atraviesa, van dejando un registro en el sobre del mensaje que se puede analizar a posteriori para identificar quien es el primer servidor de correo que ha procesado el mensaje, que debería corresponderse con el servidor del proveedor de Internet del originador del correo basura.

```
Received: from relay.upm.es(einstein.ccupm.upm.es [138.100.4.8])
        by relay.dit.upm.es (8.14.1/8.14.1) with ESMTP id m1Q9TfGr013106
        for <villagra@dit.upm.es>; Tue, 26 Feb 2008 10:29:41 +0100
Received:from tomts20.bellnexxia.net(tomts20.bellnexxia.net [209.226.175.74])
        by relay.upm.es (8.13.8/einstein-006) with ESMTP id m1Q6xCh7028938
        for <villagra@dit.upm.es>; Tue, 26 Feb 2008 07:59:18 +0100(MET)
```

En las cabeceras mostradas en las líneas anteriores, se puede comprobar que el primer mensaje es una traza interna de la organización destino (relay.dit.upm.es lo recibe de relay.upm.*es*), pero la segunda identifica el servidor de correo que ha enviado el mensaje hacia los servidores de la organización (relay.upm.*es* lo recibe de tomts20-srv.bellnexxia.net), traza fiable por ser generada por el propio servidor destinatario del mensaje. Trazas anteriores a ésta pueden haber sido falsificadas, por lo que no deben tomarse en cuenta. Tras analizar las líneas anteriores, se puede inferir que el servidor tomts20-srv.bellnexxia.net es, o el propio ordenador utilizado por el originador para enviar el correo, o el servidor de correo

que utiliza el remitente para distribuir sus mensajes. Con esta información, es posible realizar una búsqueda en Internet acerca de ese dominio para saber quién es su proveedor de Internet y poder formalizar la queja ante este abuso.

Por ejemplo, una búsqueda en un servidor del servicio whois, (www.whois-search.com) de la dirección IP del servidor tomts20-srv.bellnexxia.net (209.226.175.74) da como resultado lo siguiente:

```
OrgName:    Bell Canada
OrgID:      LINX
Address:
City:       toronto
StateProv:  ON
PostalCode: K1G-3J4
Country:    CA

NetRange:   209.226.0.0 - 209.226.255.255
CIDR:       209.226.0.0/16
NetName:    BELLCANADA-3
NetHandle:  NET-209-226-0-0-1
Parent:     NET-209-0-0-0-0
NetType:    Direct Allocation
NameServer: TOROON63NSZP05.SRVR.BELL.CA
NameServer: TOROONDCNSZS05.SRVR.BELL.CA
Comment:    ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:    1998-04-28
Updated:    2006-12-13

RTechHandle: PD135-ARIN
RTechName:   Daoust, Philippe
RTechPhone:  +1-416-215-5423
RTechEmail:  noc@in.bell.ca

OrgAbuseHandle: ABUSE1127-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-877-877-2426
OrgAbuseEmail:  abuse@bellnexia.net

OrgAbuseHandle: ABAI1-ARIN
OrgAbuseName:   Abuse Business abuse issues
OrgAbusePhone:  +1-877-877-2426
OrgAbuseEmail:  abuse@bellnexia.net

OrgTechHandle: SYSAD1-ARIN
OrgTechName:   Sys Admin
OrgTechPhone:  +1-800-565-0567
OrgTechEmail:  ip_prov@bell.ca

# ARIN WHOIS database, last updated 2008-02-26 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Cabe destacar el dato de "OrgAbuseEmail", una dirección de correo electrónico de este proveedor destinada a notificar este tipo de abusos. Si se enviara a esta dirección una copia del mensaje de correo basura recibido, con todos sus campos y cabeceras, el proveedor podría identificar adecuadamente al usuario remitente y actuar en consecuencia.

Esta forma de identificar al originador de los correos basura es conocida también por los atacantes, de forma que han ideado nuevas técnicas para poder realizar envíos masivos de correo basura sin ser descubiertos. La más utilizada consiste en aprovechar el hecho de que el protocolo SMTP no tiene autenticación lo que permite utilizar como servidor de envío de correo saliente un servidor externo, que no pertenece al proveedor de servicios del atacante, lo que complica la identificación. Esta técnica se refleja en la Figura 6.

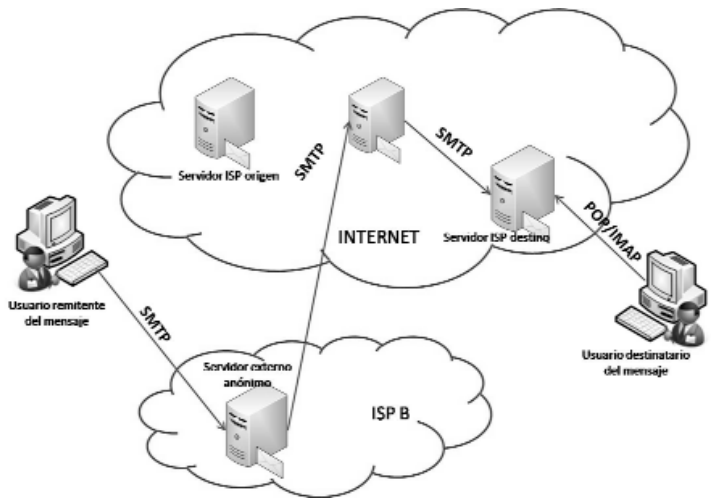

Figura 6: Uso de servidor SMTP anónimo

La utilización de servidores externos para reenvío de correo electrónico es posible teóricamente, pero constituye una mala práctica que no debería realizarse en condiciones normales. Por ello, se ha realizado una campaña en Internet para convencer a los administradores de sistemas que configuren sus servidores de correo electrónico de forma que no permitan su utilización como pasarela de envío de correo basura, es decir, no deben permitir la recepción de correo cuyo remitente y destinatario sean usuarios externos al servidor de correo. Como consecuencia de la campaña, las nuevas versiones software de los servidores restringen por defecto este

tipo de comportamiento, pero los servidores antiguos que no tienen una administración adecuada siguen siendo utilizados por los atacantes para distribuir correo basura, distribuyéndose entre ellos listas de servidores de correos abiertos que pueden utilizar. Con el fin de identificar a los servidores de correo electrónico utilizados por los distribuidores de correo basura, surgen las denominadas "listas negras" (*Black listing*, o RBL - *Realtime Blackhole List*), que son listas de servidores mal configurados que permiten el envío de correo basura, mantenidas por distintas organizaciones. La utilización de estas listas depende de cada administrador:

- Algunos administradores configuran sus servidores de correo para directamente rechazar cualquier mensaje procedente de servidores de correo incluidos en las listas negras. El problema es que este rechazo afecta a todos los usuarios legítimos de correo electrónico que utilicen dicho servidor.

- Otros administradores incluyen en sus filtros de detección de correo basura la consulta de estas listas, de manera que si un mensaje ha sido transmitido a través de un servidor incluido en ellas, se le aumenta la probabilidad de ser etiquetado como correo basura.

Esta estrategia hace que los administradores cuiden mucho la aparición de servidores de correo mal configurados en sus dominios, razón por la que los remitentes de correo basura han tenido que buscar nuevas vías, como por ejemplo, atacar sistemas e intentar instalar en sus dominios servidores de correo que permitan el reenvío de correo basura. De esta manera, crean una red de robots, que suelen ser sistemas de usuarios finales, que no tienen una correcta administración de seguridad y que sin saberlo, se han convertido en distribuidores masivos de correo basura. La única solución en este caso, es su identificación en las listas negras e intentar localizar al proveedor de Internet de estos usuarios y notificarles el problema existente.

2.2.2.5 Acceso a la información en tránsito

El último de los ataques provocados por la actividad de un usuario en Internet radica en la posibilidad de acceder a la información que el usuario envía por la red. Si el atacante tiene acceso a algún punto de la red por donde se transmite la información del usuario, esta información es vulnerable a diversos ataques, como se ve en la Figura 7.

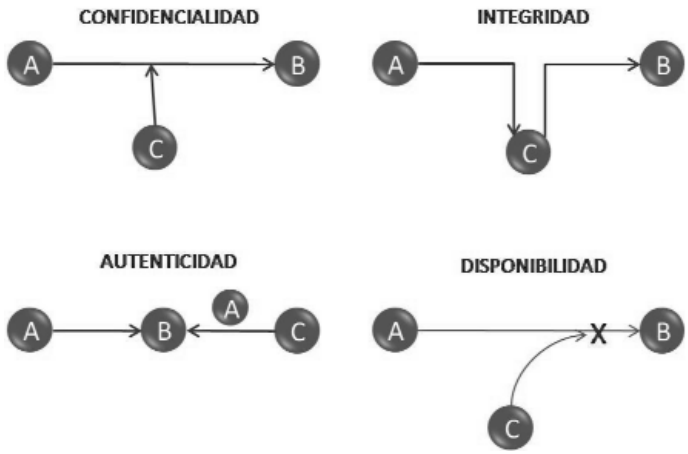

Figura 7: Ataques a la información en tránsito

Existen cinco tipos principales de ataques [12], aunque en la figura sólo se observan los cuatro primeros, ya que la representación gráfica del quinto no aporta información adicional:

- Ataque a la disponibilidad: el atacante puede eliminar la información del canal de comunicación, impidiendo que llegue a su destinatario.
- Ataque a la confidencialidad: el atacante puede escuchar en el canal de comunicación la información transmitida por el usuario.
- Ataque a la integridad: el atacante puede interceptar la información y modificarla en tránsito, enviando información alterada al destinatario.
- Ataque a la autenticidad: el atacante puede falsificar información y enviarla al destinatario haciéndose pasar por otro originador.
- Ataque de repudio: ataque específico de la información en tránsito que surge como consecuencia de los ataques anteriores:

- Repudio de envío: un atacante envía cierta información a un destinatario y posteriormente niega haber realizado dicho envío, amparándose en que ha sido un envío falso realizado por un atacante intermedio mediante un ataque a la autenticidad.

- Repudio de recepción: un atacante recibe un mensaje de un originador pero posteriormente niega haberlo recibido, amparándose en que ha sido objeto de un ataque a la disponibilidad realizado por un atacante intermedio.

Es muy complicado evitar estos ataques mediante mecanismos de defensa, ya que supondría una protección física de los medios de transmisión, lo cual en muchos casos es imposible o inviable. Por ello, es necesario asumir que toda información en tránsito puede ser atacada y tratar de plantear la defensa ante estos ataques utilizando otros mecanismos que supongan la disminución o anulación del impacto provocado por el ataque. Estos mecanismos son los denominados mecanismos de protección de la información en tránsito.

Capítulo 3

Seguridad de acceso a la red

3. Seguridad de acceso a la red

Una vez analizadas las potenciales amenazas que surgen de la conectividad y utilización de Internet, es necesario establecer un conjunto de medidas de seguridad que permitan abordar estas amenazas estableciendo, de esta forma, una política de seguridad de la organización. Como se describió en la sección 1.1, antes de implantar servicios de seguridad en la organización, es necesario estudiarlos y planificarlos adecuadamente de acuerdo a un análisis de riesgos y un estudio económico que permita identificar cuáles son los riesgos de los que una organización se debe proteger optimizando, además, la inversión económica.

Los servicios de seguridad se pueden clasificar de múltiples formas. En este texto se van a clasificar en función del activo de la empresa que se está protegiendo, distinguiendo dos grandes tipos de activos de seguridad de la organización, dependiendo de su ubicación [13]:

- Activos situados dentro del dominio de la organización, sobre los que el administrador de seguridad tiene capacidad de actuación para, por ejemplo, poder establecer políticas de defensa destinadas a disminuir sus vulnerabilidades restringiendo el acceso a estos activos. Son los servicios de Seguridad de Acceso a la Red.

- Activos ubicados fuera del dominio de la organización, y que, por tanto, no pueden ser protegidos restringiendo su acceso. Consisten principalmente en la información interna de la organización que está siendo transmitida a través de redes externas a la organización, sobre las que no se tiene capacidad de actuación para restringir el acceso a la información de la organización que se está transmitiendo. Por ello, los servicios de seguridad destinados a proteger a estos activos no pueden ser defensivos, que tratan de evitar el ataque, sino de seguro, cuyo objetivo es minimizar su impacto. Se basan en la aplicación de técnicas criptográficas para proteger la confidencialidad e integridad de la información, y se conocen como servicios de Protección a la Información en Tránsito.

En este capítulo y siguientes, se describen los servicios de seguridad de acceso a la red más relevantes.

Los servicios de seguridad de acceso a la red tienen como objetivo restringir el acceso no autorizado a los activos de las redes y sistemas de una organización. Para ello, la primera tarea consiste en identificar las vías de acceso a las entidades de la organización. Esta identificación debe incluir:

- Acceso físico a la organización: el atacante se persona físicamente dentro o cerca de la organización de forma que puede acceder a los activos de la misma. La defensa contra este tipo de ataques consiste en llevar a cabo servicios de seguridad de control de acceso físico.

- Acceso lógico a la organización: el atacante intenta acceder a los activos de la organización a través de redes externas a las que está conectada la misma. La defensa contra este tipo de ataques consiste en llevar a cabo servicios de seguridad de control de acceso lógico.

3.1 Control de acceso físico

El objetivo de estos servicios de seguridad es evitar que los atacantes accedan de forma física a los activos de la organización, ya sean sistemas informáticos, cables, armarios repartidores, redes inalámbricas, etc.

Las medidas de seguridad establecidas son las clásicas técnicas de control de acceso físico utilizadas en el campo de la seguridad civil para protección de espacios y edificios. En el caso de las redes y sistemas informáticos de una organización, lo primero que se debe realizar es identificar las zonas de seguridad cuyo acceso físico debe ser protegido, y a partir de ahí, proteger las fronteras entre zonas. Una práctica muy usual es la identificación de dos zonas:

- Zona interna: todos los equipos, sistemas, redes y componentes de la organización.

- Zona externa: el resto.

En este caso, los servicios de seguridad de control de acceso físico deben centrarse en la protección del perímetro físico donde se encuentran las instalaciones de sistemas informáticos de la organización. No obstante, pueden darse otros casos más complejos, como la existencia de zonas de invitados, zonas públicas internas a la organización, etc. En estos casos, es necesario hacer una planificación detallada de los sistemas y elementos necesarios en cada una de las zonas y proteger las fronteras entre zonas de la forma más adecuada.

Los servicios que permiten proteger físicamente las fronteras entre zonas de seguridad, y por tanto los activos de la organización incluidos en cada una de ellas, pueden incluir:

- Protección de puntos de acceso físico: puertas, ventanas, etc., protegidas de forma adecuada al nivel de seguridad exigido, mediante llaves, sistemas acorazados, apertura con identificación, vigilancia presencial, etc.

- Sistemas de vigilancia de accesos: video vigilancia, alarmas perimetrales, volumétricas, etc.

Sin embargo, existen ciertos activos que pueden traspasar los límites de las zonas de seguridad física identificadas, sin poder tener una delimitación exacta de su alcance; son los activos de la organización que se propagan por radiaciones electromagnéticas desde el interior de la organización.

La irradiación electromagnética puede ser un grave problema para los administradores de seguridad, ya que rompe todas las medidas de seguridad física establecidas. Los casos más importantes a considerar son:

- Redes inalámbricas, tales como WiFi, *Bluetooth*, etc. Dado su potencial alcance, el mayor problema práctico reside en las redes inalámbricas con WiFi. En efecto, uno de los ataques más utilizado actualmente es el denominado "ataque del aparcamiento" ilustrado en la Figura 8, en el que el atacante accede a un entorno físico cercano a la organización (como por ejemplo, el aparcamiento), situado fuera de los controles de acceso físico establecidos, y trata de escuchar la actividad de redes inalámbricas en la zona, con el fin de encontrar una red inalámbrica que pertenezca a la organización, intentar conectarse a ella, y de esta manera, ganar acceso a las redes y recursos internos de la organización, siempre que la red permita el acceso a los activos internos.

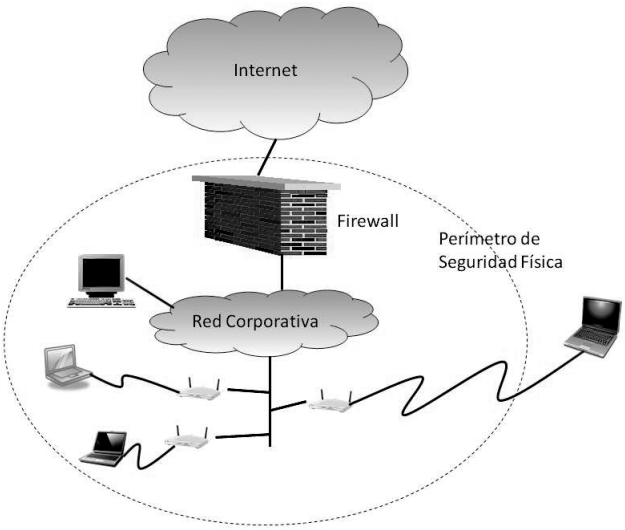

Figura 8: Ataque del aparcamiento

Este hecho, unido a las vulnerabilidades conocidas en la protección de las redes inalámbricas, hacen que en entornos críticos se desaconseje la utilización de redes inalámbricas y que, en caso de existir, sean tratadas como redes externas a la organización que no dan acceso directo a los recursos internos de la misma, siendo necesaria la identificación ante algún control de acceso lógico para poder acceder desde la red inalámbrica al interior.

- Radiaciones emitidas por los componentes de los sistemas de información. Hay diversos elementos de los sistemas de información, tales como pantallas, teclados, líneas de alimentación, etc., que emiten radiación electromagnética que aunque de baja potencia, podría ser capturada si se dispone de una antena con la sensibilidad y direccionalidad suficiente. Este es el ataque denominado TEMPEST, que debe su nombre al programa iniciado por el gobierno de EE.UU. para limitar las radiaciones electromagnéticas de los equipos y sistemas (*Transient ElectroMagnetic Pulse Emanation Standard*) [14].

La especialización y dificultad de este tipo de ataque, hace que sea considerado sobre todo en entornos muy sensibles de alta seguridad. La defensa se basa en la separación electromagnética de los elementos sensibles que puedan emitir estas radiaciones aislándolos adecuadamente con Jaulas de Faraday, de forma que fuera de estas jaulas no se puedan captar las radiaciones emitidas dentro.

3.2 Control de acceso lógico

Una vez protegido el perímetro de acceso físico mediante las medidas explicadas anteriormente, la siguiente vía de acceso a los sistemas que es necesario proteger es el acceso a través de la conexión de la organización a redes externas. Este tipo de ataque no exige una personación física, lo que lo hace más atractivo para potenciales atacantes, dado el anonimato y la falta de compromiso a la hora de llevar a cabo el ataque (nadie puede ver al atacante, en caso de detección, se detecta una máquina no una persona, etc.).

La más sencilla y rápida de las medidas de defensa contra ataques lógicos podría consistir en restringir el tráfico entrante, ya que para hacer efectivo este tipo de ataque el atacante necesita establecer una conexión con algún sistema interno, lo que hace que pueda ser sencillo discriminar el sentido del tráfico y evitar, de esta forma, el ataque.

Sin embargo, en la mayoría de las organizaciones no es viable hacer una restricción del tráfico entrante total, ya que la organización podría utilizar una conexión a redes externas para proporcionar servicios de Internet que requieren conexiones entrantes desde el exterior, tales como un servidor Web, un servidor de correo electrónico, un servidor de acceso remoto, etc. Por ese motivo, se distinguen dos tipos de controles de acceso, necesarios para garantizar un adecuado control de acceso lógico a los sistemas de la organización:

- Restricción de tráfico no permitido: se puede bloquear el tráfico de conexiones entrantes (o salientes) que no tengan cabida en la política de provisión y acceso a servicios de la organización, en el punto adecuado de la misma. Los sistemas que permiten este tipo de restricción se denominan "Sistemas de Defensa Perimetral", ya que actúan en el perímetro de los sistemas o redes de la organización bloqueando el tráfico no permitido que intenta atravesarlo.

- Restricción de tráfico permitido: será necesario restringir las conexiones entrantes o salientes destinadas a servicios que sí están contemplados en la política de seguridad de la organización, para su utilización lícita por los usuarios autorizados, bloqueando su uso por otros usuarios no autorizados. Los sistemas que permiten este tipo de restricción se denominan "Sistemas de Autenticación y Autorización", y son normalmente utilizados también como defensa interna ante posibles usos maliciosos por parte del personal propio de la organización.

En los siguientes capítulos se analizan en detalle los distintos servicios de control de acceso lógico.

Capítulo 4

Sistemas de autenticación y autorización

4. Sistemas de autenticación y autorización

Tal y como se ha visto en el capítulo anterior, dentro del entorno de control de acceso a los activos de la organización, es necesario establecer dos vías de actuación: restringir los accesos externos a los servicios ofertados, y filtrar el resto de accesos externos (defensa perimetral). En este capítulo se estudiará la primera vía de actuación.

Los servicios proporcionados por una organización pueden ser:

- De uso anónimo, utilizables por cualquier usuario. Estos servicios no necesitan identificar al usuario que los utiliza, por lo que son más vulnerables a amenazas de seguridad. Ejemplos de estos servicios son los servidores Web, servidores de correo electrónico (protocolo SMTP), servicios de FTP anónimo, etc.

- De uso restringido para usuarios autorizados. En este caso, es necesario que el servicio lleve a cabo una identificación de los usuarios que quieren acceder a él, por lo que surge el problema de la autenticación remota de los usuarios. Es necesario utilizar algún tipo de técnica que permita tener garantía de la identidad del usuario remoto. Son las denominadas técnicas de autenticación, que permiten identificar al usuario remoto, y que pueden combinarse con sistemas de autorización, para delimitar la utilización de recursos por parte de cada usuario, según lo defina el administrador.

Por ello, es necesario establecer en detalle los mecanismos y tecnologías de autenticación que se van a utilizar para controlar el acceso a servicios de uso restringido de la organización.

La autenticación de usuarios remotos no es tan sencilla como la autenticación de seres humanos. Los seres humanos nos reconocemos físicamente cuando nos vemos, siendo esta la mejor garantía de autenticación. Pero si no hay contacto físico y la autenticación se hace remotamente, el nivel de garantía decrece bastante. Se puede realizar de la misma forma, con un reconocimiento físico, pero a distancia, enviando los datos físicos del usuario remoto para que el sistema lo pueda comprobar. Esta es la denominada autenticación biométrica. El problema radica en que este método exige la utilización de dispositivos muy específicos que permiten captar los datos físicos de los usuarios y transmitirlos a través de las redes de comunicación. Por ello, se han desarrollado otros sistemas más simples que permiten llevar a cabo la autenticidad de los usuarios remotos, aunque esto suponga una leve disminución de la garantía de éxito.

El principal método es la compartición de un secreto entre el usuario remoto y el servidor. Este secreto puede ser:

- Algo que se sabe, y que sólo lo debe saber el usuario remoto.

- Algo que se tiene, y que sólo lo debe tener el usuario remoto.

- Algo que se es, peculiar y específico del usuario remoto.

Por otra parte, un mecanismo adicional a la compartición del secreto, es la localización del usuario remoto, de forma que si se tiene alguna garantía de que sólo el usuario remoto puede acceder a una localización, las conexiones que provengan de dicha localización sólo pueden ser realizadas por dicho usuario remoto, permitiendo una cierta garantía de su identidad. No obstante, este método es muy vulnerable a ataques y no se suele utilizar como único método de autenticación de usuarios, sino que suele combinarse con otros.

Antes de detallar los métodos de autenticación, es conveniente conocer de qué forma el usuario remoto y el servidor comparten el secreto. Para ello, es necesaria una fase previa de registro en la que, por medio de algún mecanismo, el usuario remoto le comunica al servidor su secreto. El servidor puede imponer restricciones a la hora de permitir el registro de usuarios, de forma que se eviten suplantaciones de identidad en el registro. Por ejemplo, para ciertos tipos de servicios se exige un registro con personación física que permita la identificación biométrica del usuario; en otros servicios, se impone una vía de comunicación alternativa para el registro de manera que existan más datos que garanticen la identidad real del usuario (como por ejemplo verificación del registro por correo electrónico o por correo postal). Una vez que el servidor posee el secreto del usuario, puede autenticarlo cada vez que intente acceder a él.

A continuación, se describen los principales mecanismos de autenticación de usuarios.

4.1 Sistemas de autenticación biométrica

Se trata de sistemas que tratan de emular la autenticación realizada por los seres humanos, mediante el reconocimiento de rasgos físicos característicos [15]. El principal problema de estas técnicas aplicadas a la autenticación de usuarios remotos a un servicio, es la necesidad de disponer de periféricos adecuados en los sistemas informáticos remotos que permitan capturar la información biométrica necesaria.

Los principales rasgos biométricos que pueden ser utilizados se dividen principalmente en características físicas y características de comportamiento.

4.1.1 Características físicas

Cada persona tiene un conjunto de características físicas inherentes, que cambian normalmente debido al proceso natural de evolución de las personas, y no en un período corto de tiempo. Son específicas de cada persona (no existen dos personas que tengan todos sus rasgos idénticos). Además, los periféricos utilizados capturan los rasgos de los usuarios con un nivel de precisión muy alto, lo que hace muy difícil encontrar dos personas que posean un rasgo idéntico si se utiliza esta técnica de autenticación. Las características más utilizadas son:

- Características relacionadas con los ojos:

  - Reconocimiento de retina: los primeros sistemas de autenticación biométrica se basaban en la identificación de los capilares existentes en la retina, que se consideran propios e individuales de cada persona. Sin embargo, la captura resultaba complicada e incómoda para el usuario, ya que este mecanismo se basa en el uso de haces de luz infrarroja a corta distancia del ojo del usuario.

  - Reconocimiento de iris: más recientemente, se ha identificado el iris como una fuente de gran cantidad de información propia e individual de cada persona. La captura de datos es más amigable que en el caso de la retina, ya que sólo es necesaria una "foto" del iris del usuario. Este método es menos invasivo que la exposición a infrarrojos.

- Características relacionadas con las manos:

  - Huella dactilar: las yemas de los dedos contienen un conjunto de pequeños pliegues que forman un patrón de crestas y valles que se mantiene constante a lo largo de la vida de las personas, siendo muy poco probable que coincida en dos personas si se obtiene con la precisión suficiente. La captura de la huella digital es una técnica muy cómoda y barata, ya que con un pequeño sensor que lleve incorporado un escáner de huella se puede obtener el patrón necesario para la autenticación. Por esa razón, este método es el más extendido actualmente dentro de la autenticación biométrica.

- Geometría de la mano: la forma de la mano, el tamaño de la palma y las formas de los dedos, son también datos que pueden ser utilizados para identificar a cada persona. Sin embargo, es un método que no se utiliza demasiado al necesitar un periférico de mayor tamaño (escáner del tamaño de la mano) y estar sujeto a problemas prácticos de utilización (uso de anillos, traumatismos, etc.).

• Características relacionadas con el rostro:

- Reconocimiento facial: se trata de utilizar el mismo mecanismo que usamos los seres humanos para la identificación mutua, el reconocimiento de las caras. En este caso, el usuario remoto utilizará un dispositivo (fotografías, vídeos, etc.) que le permita captar las principales características de su rostro y enviarlas al extremo remoto para que lo pueda comparar con el patrón de rostro almacenado previamente. El problema reside en que se trata de un mecanismo muy complejo, ya que es necesario un minucioso y costoso proceso para extraer los datos identificativos del rostro a partir de una fotografía que permita compararlo con los patrones. Por esta razón, no tiene demasiada utilidad en autenticación remota de usuarios de red, aunque sí es muy utilizado en otros ámbitos de seguridad civil y de defensa, tales como la identificación de sospechosos en determinadas zonas de paso (aeropuertos, etc.), sobre todo a partir de los atentados terroristas de Nueva York del 11 de Septiembre del 2001. Es por ello, por lo que el avance en I+D realizado en estos ámbitos, puede extrapolarse, en un futuro, a su uso en autenticación remota en red.

• Características genéticas:

- ADN: todas las formas de autenticación biométrica expuestas anteriormente están sujetas a un determinado margen de error debido a que es necesario un gran nivel de detalle en la captura de datos para tener la confianza de que no se van a producir identificaciones erróneas, partiendo del hecho de que dos personas pueden tener rasgos biométricos muy similares. El único rasgo biométrico que puede garantizar una identificación totalmente fiable es el ADN. Sin embargo, se trata de un método que plantea grandes inconvenientes prácticos, debido a la complejidad de realizar una identificación de ADN actualmente (solo realizable en laboratorios químicos), unido a los problemas relacionados con la privacidad que puede plantear la información adicional que se puede extraer del ADN de una persona (enfermedades, defectos congénitos, etc.).

4.1.2 Características de comportamiento

Las técnicas anteriores se basan en la captura de características físicas de las personas, y por lo tanto, estáticas. Pero existen otro tipo de características dinámicas que permite identificar a los seres humanos, aunque con una garantía de éxito menor, por lo que las técnicas basadas en el análisis de este tipo de características deben ser usadas en combinación con otro tipo de técnicas y nunca en solitario. Estas técnicas son:

- Reconocimiento de voz: se trata de una combinación de características físicas estáticas y de comportamiento dinámicas. El timbre de la voz es una característica física, pero la entonación, graduación, volumen y otras características de la voz son características dinámicas que dependen del estado de la persona. Por ello, son sistemas vulnerables a falsos positivos (imitación de la voz de otra persona) y falsos negativos (alteraciones de la voz propia debida a un resfriado, etc.), por lo que su uso debe realizarse en combinación con otras técnicas de autenticación.

- Reconocimiento del ritmo de tecleo: otro rasgo característico de cada ser humano es el ritmo de pulsaciones en el teclado. Científicos han demostrado que cada persona tenemos un ritmo de pulsaciones particular, que puede contribuir a la identificación más certera de la persona. Sin embargo, no debe usarse como único modo de identificación ya que es susceptible a múltiples variaciones (uso de distintos teclados, daños en algún dedo, etc.). Uno de los métodos más utilizados es usar esta técnica para introducir una clave de seguridad, junto con la seguridad de secreto compartido que proporciona la propia clave. Este método consiste en extraer el ritmo de pulsación de dicha clave y compararlo con el ritmo habitual de pulsación de la misma. El hecho de tener que utilizar la clave todos los días hace que al final cada usuario la introduzca de una forma semiautomática y con un ritmo totalmente predefinido. En caso de que un atacante haya capturado la clave de otra persona y la introduzca en un teclado, el ritmo de pulsación va a ser totalmente distinto del ritmo del verdadero propietario, por lo que este método permite identificar potenciales anomalías en la introducción de claves.

4.2 Sistemas de autenticación por clave

Una de las principales limitaciones de la utilización de los sistemas de autenticación biométrica es la necesidad de utilizar periféricos específicos para capturar los rasgos biométricos de los usuarios. Por este motivo, queda patente la necesidad de otro tipo de sistemas de autenticación de usuarios remotos. El sistema más utilizado de autenticación remota es el del secreto compartido o autenticación por clave, que no necesita ningún tipo de periférico.

En este sistema, el usuario genera un secreto que comparte con el sistema en la denominada fase de registro. Posteriormente, en la fase de acceso, el usuario remoto proporciona el secreto compartido, que el sistema comparará con el que tiene registrado, permitiendo o denegando el acceso consecuentemente. Se trata del método más simple y barato, ya que solo se necesita un teclado o un ratón para la introducción del secreto compartido. Sin embargo, está expuesto a múltiples riesgos:

- Ataques al repositorio de claves.
- Ingeniería social.
- Captura de la introducción.
- Adivinación.
- Captura en línea.

A continuación se detallan cada uno de estos riesgos en detalle.

4.2.1 Ataques al repositorio de claves

Durante la fase de registro (1), el usuario introduce su secreto compartido en el sistema al que se quiere autenticar posteriormente. Este sistema debe almacenar las claves de los usuarios en algún repositorio (2) para, posteriormente, poder compararlas con las proporcionadas remotamente por los usuarios cuando sea oportuno. Este repositorio de claves contiene una información muy sensible, siendo por ese motivo vulnerable a un ataque. Un ataque al repositorio de claves (3) permitiría a un atacante obtener directamente las claves secretas de todos los usuarios del sistema (4). La Figura 9 muestra el proceso seguido durante la fase de registro si se almacenan las claves en claro, donde se observa claramente cómo los atacantes pueden acceder a la información almacenada en el repositorio.

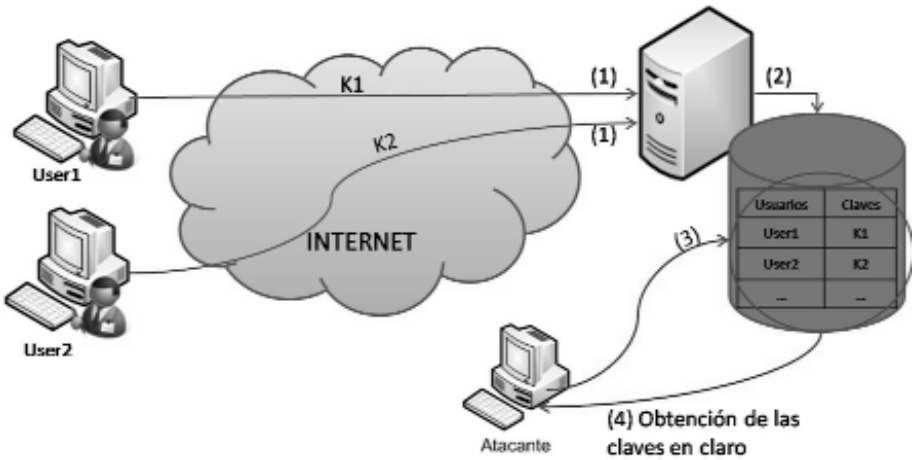

Figura 9: Registro de claves en claro. Ataque al repositorio de claves

En la figura se observa que el sistema almacena la clave en claro en la fase de registro, por lo que cuando posteriormente el usuario proporciona la clave remotamente en la fase de acceso, el sistema sólo tiene que compararla con la clave almacenada. Este sistema es vulnerable, como se ha comentado en los párrafos anteriores, a un ataque al repositorio de claves que permitiría obtener todas las claves de usuario almacenadas.

Por el problema anterior, es necesario que el sistema remoto no almacene las claves de los usuarios en un formato accesible por los atacantes o por los propios usuarios locales del sistema. Una buena solución al problema consiste en utilizar un almacenamiento cifrado de las claves de los usuarios.

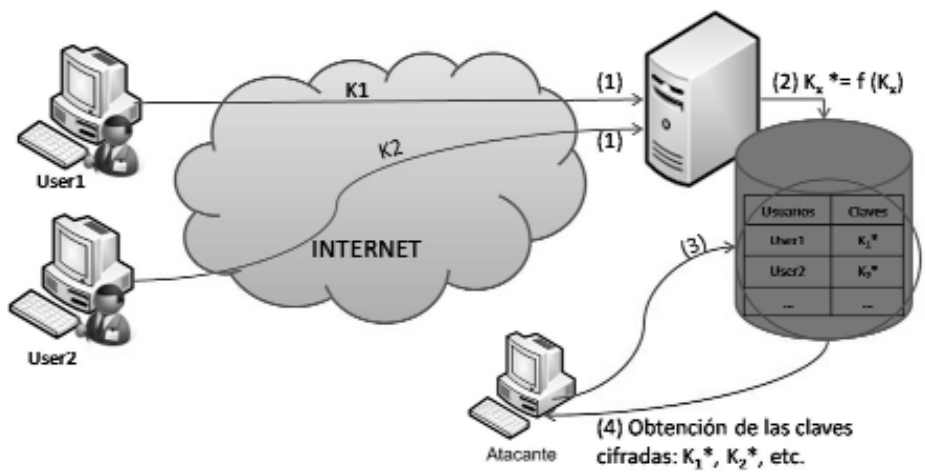

Figura 10: Registro de claves cifradas. Ataque al repositorio de claves

En la Figura 10, se muestra el proceso de almacenamiento en la fase de registro cuando se realiza un cifrado de claves. Para ello, se utilizan funciones de cifrado de las denominadas de un único sentido, es decir, funciones que se pueden aplicar en un sentido pero no se conoce la función inversa que permita descifrar la información. Esto las convierte en funciones útiles en este entorno, ya que si un atacante accede al repositorio de claves cifradas no tiene forma de conocer las claves reales utilizadas por los usuarios.

El proceso seguido, tal como se muestra en la Figura 11, es el siguiente: la clave elegida por el usuario para autenticaciones posteriores es cifrada en la fase de registro y almacenada en forma cifrada. Cuando el usuario remoto quiere acceder a algún servicio del sistema, proporciona la clave de usuario registrada anteriormente. En este momento, el sistema debe comparar la clave introducida con la clave almacenada en el registro, para lo que deberá aplicar la misma función de cifrado que utilizó para cifrar la clave en la fase de registro a la clave proporcionada remotamente por el usuario, y comparar las dos versiones cifradas de las claves. En caso de que ambas claves coincidan, el sistema permitirá el acceso del usuario remoto al sistema; en caso contrario, le denegará el acceso.

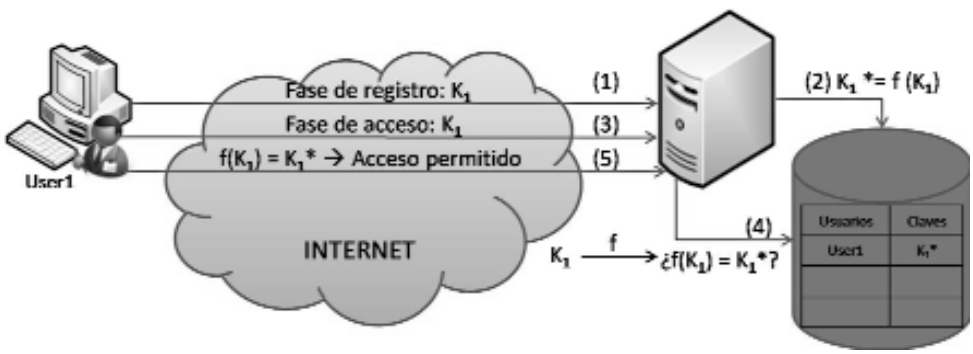

Figura 11: Mecanismo de autenticación por clave. Fases de registro y de acceso

La Figura 12 muestra un ejemplo de repositorio de claves cifradas en sistemas UNIX, en los que el segundo campo (separados con ":") contiene la versión cifrada de las claves[1].

```
lpr01100:OJvg4HVqbF8ek:10100:10000:SANCHEZSANCHEZ,PEDRO,15000,:/users/cuentas/lpr01100:/dev/null
lpr01101:CONJGtHK0JgCo:10101:10000:PEREZ PEREZ, JUAN,15000,:/users/cuentas/lpr01101:/dev/null
lpr01102:JDFg4X99.T/vs:10102:10000:GOMEZ GOMEZ, LUIS,15000,:/users/cuentas/lpr01102:/dev/null
lpr01103:HKyftkVWFO4pU:10103:10000:SANZ SANZ, ANA,15000,:/users/cuentas/lpr01103:/dev/null
lpr01104:KNb3KVyGWIKe2:10104:10000:RUIZ RUIZ, JOSE,15000,:/users/cuentas/lpr01104:/dev/null
```

Figura 12: Repositorio de claves cifradas en UNIX

4.2.2 Ataques de ingeniería social

Como se expuso en el capítulo anterior, el punto más débil de la cadena suele ser el propio usuario, especialmente cuando no tienen una gran familiarización con las tecnologías. Esta vulnerabilidad puede ser utilizada por un atacante para intentar conseguir la clave de los usuarios. Existen múltiples métodos para intentar engañar al usuario, que van desde las llamadas telefónicas haciéndose pasar por el departamento de sistemas de la organización y solicitando la clave (ataque que sorprendentemente tiene un alto grado de éxito), hasta engaños más sofisticados que consisten en falsificar al sistema remoto y encaminar al usuario hacia el nuevo sistema falsificado, donde el usuario introducirá su clave que será capturada.

Es muy difícil evitar este tipo de ataques utilizando medios técnicos, ya que son ataques a la ingenuidad y falta de conocimientos de los usuarios. Por ello, el mejor método de defensa contra estos ataques consiste en educar a los usuarios y realizar campañas de concienciación. Es necesario recordar continuamente a los usuarios que nadie legítimo les va a solicitar las claves por ningún medio que no sea el propio sistema remoto al que se deben conectar, que deben desconfiar de mensajes que informen de fallos de seguridad e induzcan al usuario a introducir sus claves en una cierta dirección, etc.

[1]El almacenamiento de las claves cifradas en sistemas UNIX cuenta con un grado de seguridad adicional, al añadir el denominado "*salt*" (los dos primeros caracteres de la versión cifrada de la clave) a la clave cifrada. Este complemento permite generar 4096 distintas versiones de la clave cifrada, dependiendo del "*salt*" usado, y protegiendo el repositorio de ataques de comparación con listas de claves ya cifradas.

4.2.3 Ataques de captura de la introducción

Otro mecanismo para capturar claves de usuarios es la observación durante su introducción en el teclado. Las personas que estén físicamente próximas al usuario podrán observar las pulsaciones de éste cuando introduce su clave y así obtenerla. Aunque este ataque solo es útil cuando se está físicamente cercano al usuario, lo que reduce el ámbito y número de posibles atacantes, resulta conveniente señalar algunas normas de "buena educación informática" para intentar evitarlo. Por ejemplo, en los momentos en los que se está reunido con un compañero y éste debe introducir una clave, es una buena costumbre que las personas que le rodean aparten la vista del teclado de una manera ostensible (por ejemplo, apartándose, mirando por la ventana, etc.), y permitan al usuario introducir su clave con un cierto grado de comodidad. Nuevamente, la defensa contra este tipo de ataques consiste en educar a los usuarios e inculcarles un conjunto de buenas costumbres a realizar en estos casos [16].

4.2.4 Ataques de adivinación

Este tipo de ataque es uno de los más problemáticos respecto a la utilización de claves por los usuarios. Como se vio anteriormente y quedó reflejado en la Figura 10, el hecho de que un atacante pueda acceder al repositorio de claves de usuarios de un sistema provoca que sea necesaria cifrar las claves en dicho repositorio y mantener el repositorio con versiones cifradas de las claves. Sin embargo, todos los cifrados son susceptibles a los denominados ataques de fuerza bruta, que consisten en probar todas las posibilidades hasta dar con una clave cuya versión cifrada es igual a la almacenada en el repositorio. Este ataque es siempre factible, por lo que la única defensa que se tiene contra este ataque es hacer que el tiempo necesario para probar todas las claves posibles sea tan elevado que no sea realizable en condiciones normales. Para ello, es necesario aumentar el número de posibles claves hasta una determinada magnitud que haga impracticable un ataque de fuerza bruta.

Aumentar el número de posibles claves se consigue aumentando su longitud. Por ejemplo, una clave de 4 dígitos, como la mayoría de los PIN utilizados en los cajeros bancarios, da lugar a un conjunto de 10.000 posibles claves, muy fácil de probar en un tiempo prudencial utilizando un ordenador. Si se analizan las claves utilizadas actualmente en los sistemas, gran parte de ellas están formadas por 8 símbolos. Si cada símbolo se representa mediante código ASCII simple con 7 bits, se obtienen claves de 56 bits, lo cual da lugar a un universo de 2^{56} posibles claves, es decir, 72.057.594.037.927.936 posibles claves (más de setenta dos mil billones de posibles claves). Esta cantidad es suficientemente elevada

para hacer poco práctico gran cantidad de los ataques de fuerza bruta básicos, por lo que en principio se puede considerar que una clave de 8 símbolos es suficientemente segura frente a ataques básicos de fuerza bruta.

Sin embargo, la anterior asunción sólo es cierta en el caso de que las 2^{56} posibles claves sean equiprobables, es decir, que un usuario elija aleatoriamente una de ellas. Pero esto no es cierto, ya que los usuarios no eligen aleatoriamente 56 bits, sino 8 símbolos, que además deben recordar fácilmente, por lo que suelen utilizar unos símbolos más que otros. Por ejemplo, las claves contienen muchos más símbolos de letras minúsculas que mayúsculas, más símbolos de letras que de números, más símbolos alfanuméricos que de otro tipo de símbolos. Por estos motivos, la elección de las claves no es aleatoria, sino que hay claves más probables que otras. Prueba de ellos es que resulta mucho más sencillo encontrar claves como "maria14" que "%P=9@]T<". Por ello, los ataques de fuerza bruta a repositorios de claves no se basan en probar todas las posibles combinaciones de símbolos que generan claves de 56 bits, sino sólo las más probables, lo cual reduce drásticamente el conjunto de claves a probar, reduciendo de esta forma el tiempo de ejecución del ataque y aumentando su viabilidad y efectividad.

Estudios realizado sobre el grado de aleatoriedad de las claves de los usuarios han demostrado que, en media, de las 2^{56} posibles claves, sólo se utilizan en realidad 2^{19}, por lo que el conjunto de claves a probar en un ataque de fuerza bruta se reduce a 2^{19} (524.288), con grandes probabilidades de éxito.

Este tipo de ataques de fuerza bruta que consiste en probar un determinado subconjunto de posibles claves, se denominan "ataques de diccionario". Se llaman así debido al hecho de que gran parte de las claves elegidas por los usuarios son claves iguales o derivadas de palabras pertenecientes a las distintas lenguas existentes, que como tales aparecen en diccionarios, por lo que estos ataques se basan en grandes listas de palabras, obtenidas a partir de diccionarios (88431 entradas en el diccionario de la Lengua Española de la Real Academia Española). El atacante irá cifrando palabra a palabra del diccionario y comparándola con la versión cifrada de la clave que queremos adivinar. Este tipo de ataque puede ser mejorado posteriormente aplicando variaciones a las palabras de diccionario:

- Palabras escritas al revés.

- Variaciones de mayúsculas en la primera letra.

- Adición de 1 o 2 números al final de la palabra.

- Sustitución de vocales por números, la o por 0, la i por 1, etc.

Existen múltiples programas disponibles en Internet que permiten realizar estos ataques contra un repositorio de claves cifradas, permitiendo incluso cargar diccionarios de diferentes idiomas y programar las variaciones de claves que se quieren aplicar. Pruebas realizadas han demostrado que en un entorno típico de usuarios, no necesariamente técnicos, el 25% de las claves eran adivinadas en menos de 2 horas mediante el uso de estos programas.

La defensa frente a este tipo de ataques se basa nuevamente en la educación de los usuarios y en la concienciación de éstos en elegir buenas claves que sean resistentes a un ataque de adivinación. Es necesario informar a los usuarios de los posibles peligros derivados del uso de claves débiles y recomendarles recetas básicas para que hagan una buena elección de sus claves, como por ejemplo:

- Mezclar letras (mayúsculas y minúsculas), dígitos y símbolos.

- NUNCA utilizar una palabra que aparezca o pueda derivarse de un diccionario (patata, pepeloli, laura15, etc.).

- Utilizar claves fácilmente recordables, para no tenerlas que llevar apuntadas en un papel.

Sin embargo, hay que asumir que por mucha concienciación que se realice, existe un elevado porcentaje de usuarios que eligen claves débiles y adivinables, lo que hace necesario el empleo de técnicas que permitan reducir el impacto de un posible ataque. Algunos métodos técnicos utilizados son:

- Uso de un repositorio de claves cifradas privado, oculto o de difícil acceso. El ataque de adivinación se basa en el acceso al repositorio de claves cifradas, por lo que si este repositorio está protegido para usuarios no administradores, se disminuye el riesgo de ataque.

- Mecanismo de control de claves. Cuando el usuario elige una clave y la almacena en el sistema durante la fase de registro, el sistema puede hacer una pequeña y rápida validación de la clave para comprobar su debilidad:

  - Ejecutar una versión básica de ataque de diccionario contra esa clave.

  - Forzar que la clave deba contener distintos tipos de símbolos (letras mayúsculas, minúsculas, dígitos, símbolos, etc.) y posea una determinada longitud.

- Mecanismo de caducidad de claves. Se trata de minimizar el tiempo de exposición de claves adivinadas o adivinables, obligando al cambio periódico de las claves. La elección del periodo de cambio adecuado es complicada, ya que periodos de caducidad largos (1, 2 años) implican una exposición muy larga de claves débiles, y periodos cortos (1 mes) pueden incomodar a los usuarios, que deben pensar y elegir claves fuertes todos los meses, provocando situaciones indeseadas como secuenciación de claves (pepeEnero, pepeFebrero, pepeMarzo, etc.).

- Debe ser inviable realizar un ataque de adivinación remotamente, sin tener acceso al repositorio de claves cifradas. Normalmente, esto se consigue limitando el número de intentos de accesos remotos erróneos al sistema.

4.2.5 Ataques de captura en línea

El último de los riesgos analizados al que se enfrentan los sistemas de autenticación basados en claves, consiste en capturar la clave cuando está siendo transmitida desde el usuario remoto hasta el sistema. Un atacante que tenga acceso físicamente al medio de transmisión puede monitorizar la línea y capturar la clave en el momento de su transmisión.

Para evitar este ataque, la defensa más efectiva consiste en no enviar las claves en claro por la línea, sino cifradas con algún mecanismo de cifrado acordado y negociado entre el terminal del usuario remoto y el sistema. Sin embargo, este método de envío de claves cifradas es factible y se puede realizar en servicios diseñados actualmente que ya tienen en cuenta el problema de la seguridad en su diseño, pero no es posible llevarlo a cabo en servicios muy utilizados actualmente pero diseñados en momentos en los que la seguridad no tenía la relevancia que posee hoy. Ejemplos de este último tipo de servicios diseñados sin tener en cuenta aspectos de seguridad que incluyen la transmisión de las claves en claro, son el protocolo de recuperación de correo electrónico POP3, los servicios Telnet y FTP, etc.

Si se quieren utilizar estos servicios de una forma segura en la transmisión de la clave, es necesario aplicar un "parche" que permita la introducción de una capa que cifre la transmisión en dichos servicios. Estos parches son los denominados envoltorios de cifrado de sesión.

Al utilizar estos envoltorios, se modifica la estructura tradicional de la torre de protocolos de estos servicios, incluyendo una nueva capa entre el protocolo de aplicación y el protocolo de transporte que realiza el cifrado

de las comunicaciones. El principal inconveniente de esta técnica es que se trata de un método no estándar, por lo que es necesario asegurar que se soporta tanto en los clientes como en los servidores.

La Figura 13 muestra un ejemplo de acceso del protocolo POP3 con la arquitectura original y otro con una torre de protocolos modificada para incluir un envoltorio de seguridad.

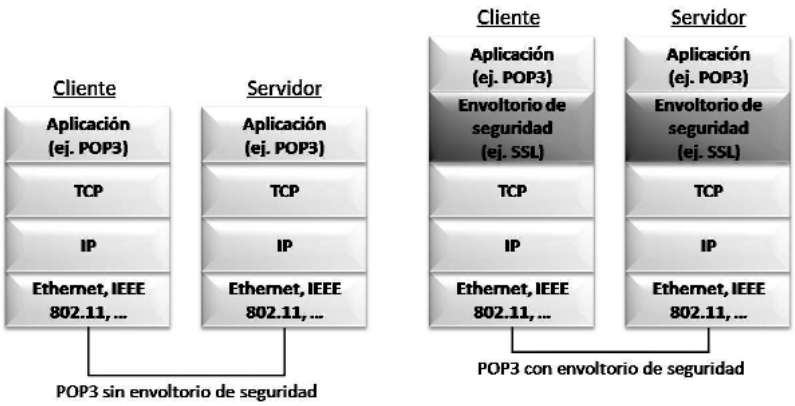

Figura 13: Envoltorios de seguridad

Muchos de los servidores de estos servicios implementan un acceso dual, con envoltorio de seguridad y sin él, para permitir las conexiones de todo tipo de clientes. Por otra parte, muchos de los clientes más utilizados también permiten la configuración con envoltorio de seguridad para su utilización en entornos en los que se dispone de un servidor que incorpora un envoltorio de seguridad. La Figura 14 muestra el soporte que da el popular cliente de correo electrónico Outlook de Microsoft para configurar la recuperación de correo con el protocolo POP3 utilizando un envoltorio de seguridad.

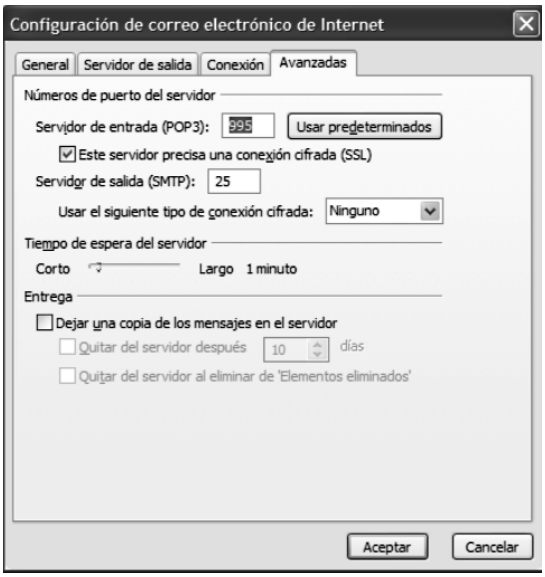

Figura 14: Recuperación de correo con POP3 con envoltorio de seguridad

El envoltorio de seguridad más popular actualmente se basa en la utilización del protocolo SSL entre el protocolo de transporte y el protocolo de aplicación. Los estándares ya prevén la utilización del protocolo SSL como envoltorio de seguridad para la mayoría de los servicios, siendo muchos los servicios que pueden apoyarse en él, como Telnet, IMAP, POP3, FTP, NNTP, SMTP, etc.

4.3 Sistemas de autenticación dinámica

El uso de envoltorios de seguridad para evitar la transmisión en claro a través de la red de las claves de los usuarios, sólo puede realizarse en una situación en la que tanto el terminal del usuario como el servidor al que se accede soporten la utilización de estos envoltorios. Existen muchas situaciones en las que no es posible usar estos envoltorios, y es necesaria la utilización de los servicios clásicos sin cifrado de claves en la red:

- Uso de terminales ajenos o terminales compartidos, cuyas aplicaciones cliente son básicas sin incluir soporte de envoltorios de cifrado.

- Acceso a servidores que no soportan envoltorios de cifrado.

Además, si se utilizan terminales ajenos aparece, en consecuencia, otro riesgo de seguridad muy grave, la captura de la clave en el propio terminal. Existen múltiples programas y aplicaciones que se instalan de forma transparente y oculta en los terminales y permiten grabar toda la actividad que el usuario realiza en dicho terminal, incluyendo las claves que introduce. Por ello, aunque el sistema incluya envoltorios de cifrado que protegen las claves en la transmisión, la utilización de terminales ajenos implica el riesgo de que la clave sea capturada en el propio terminal, anulando la funcionalidad y utilidad de los envoltorios de cifrado.

En sistemas en los que se tienen clientes estándares sin envoltorios de cifrado o terminales ajenos potencialmente inseguros, la única alternativa válida es la utilización de los denominados sistemas de autenticación dinámica. Estos sistemas se basan en el envío de claves de una forma estándar, en claro e introducidas en terminales inseguros, por lo que pueden ser capturadas fácilmente. Con el fin de minimizar el impacto de esta captura, se introducen mecanismos de variación de claves de forma que cada clave es utilizable una sola vez, son claves de usar y tirar. En estos casos, la captura de la clave es inútil ya que no tiene validez en accesos posteriores al sistema remoto.

Los sistemas de autenticación dinámica exigen que tanto cliente como servidor compartan un mecanismo de variación de claves previamente establecido entre ellos. En las siguientes secciones se presentan los principales mecanismos de autenticación dinámica.

4.3.1 Funciones encadenadas

Este tipo de sistema de autenticación dinámica consiste en algoritmos que utilizan una función criptográfica de un solo sentido "f" para generar claves de un solo uso a partir de una clave maestra inicial. Es decir, el usuario elige una clave maestra "k" y a partir de ella se generan "n" claves utilizando la función "f". La siguiente figura muestra como generar 100 claves a partir de una clave maestra dada.

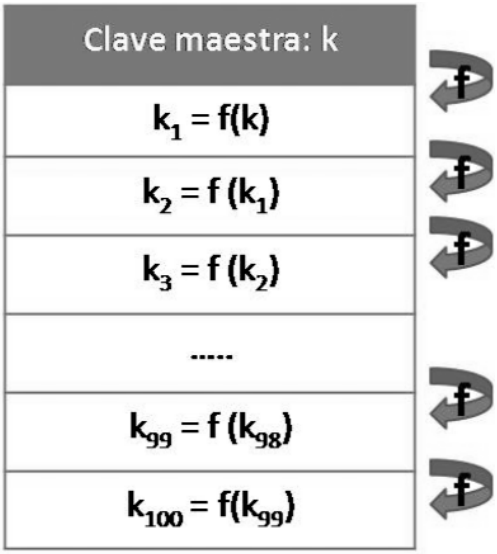

Figura 15: Generación de 100 claves de un solo uso. Funciones encadenadas

Estas "n" claves son generadas a priori y se ponen a disposición del usuario para su utilización en accesos remotos posteriores. El servidor sólo almacena, en un principio, la última clave generada (en este caso k_{100}),para evitar ataques al repositorio de claves, que permitan obtene todas las claves generadas.

Cuando el usuario accede al servicio remotamente, el servidor le solicita la clave inmediatamente anterior a la que tiene almacenada, y comprueba si la clave almacenada es función de la clave proporcionada remotamente. Si es así, el servidor le da acceso al usuario, y sustituye la clave que tiene en el repositorio por la clave proporcionada por el usuario (en el caso anterior, sustituye la clave k_{100} por k_{99}). De esta forma, en el siguiente acceso el servidor solicitará la clave anterior (k_{98}) y realizará la comprobación con la clave k_{99}, siguiendo el mismo proceso que en el caso anterior.

La Figura 16 muestra el proceso que se realiza:

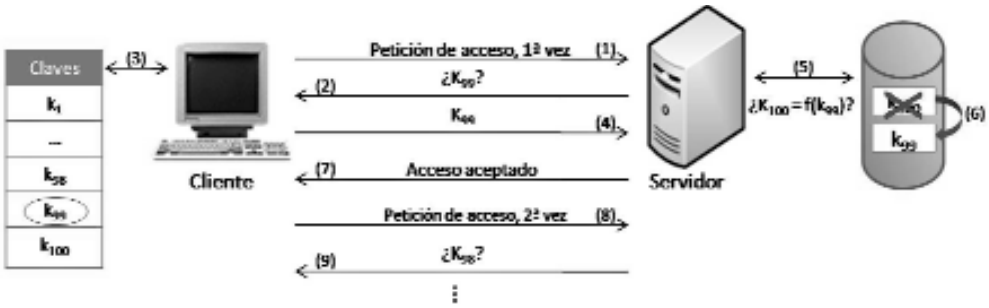

Figura 16: Autenticación dinámica. Funciones encadenadas

El mecanismo de las funciones encadenadas es un método seguro contra la captura de claves, principalmente por dos motivos. El primero de ellos es el hecho de que a pesar de que un atacante capture una clave, no puede volver a utilizarla ya que pierde su validez en el primer uso. Por otra parte, capturar una o varias claves no aporta al atacante información que le permita deducir las siguientes claves, ya que se solicitan en orden inverso al de su generación, y al ser generadas mediante una función de un solo sentido, no es posible deducir una clave a partir de claves posteriores.

Sin embargo, a pesar de lo anterior, este método adolece de inconvenientes prácticos que lo hacen poco útil en sistemas reales:

- Es necesario un acuerdo previo con el sistema remoto para generar las "n" claves. Cada vez que se gastan las claves generadas y se quieren generar de nuevo, se tiene que establecer un nuevo acuerdo.

- Y, más importante, es necesario que el usuario disponga de algún mecanismo para guardar las claves que debe utilizar. Este mecanismo puede ser desde un papel impreso (muy barato, pero altamente desaconsejable dados los riesgos de pérdida, robo, etc.), hasta una tarjeta inteligente en la que se almacenen las claves o se genere dinámicamente la clave que se tiene que utilizar en cada momento, a partir de la introducción de la clave maestra y el número de clave que se quiere utilizar. Este método es más seguro que el del papel impreso, pero resulta más caro ya que hay que proporcionar a todos los usuarios las tarjetas inteligentes.

4.3.2 Claves dependientes del tiempo

Para paliar el inconveniente de tener que generar ad-hoc la lista de claves cada vez que se agotan, surgen otros sistemas de autenticación dinámica que tratan de evitarlo. El más utilizado es el sistema de claves dependientes del tiempo, en el que tanto el usuario como el servidor conocen un mecanismo de variación de claves que son función del tramo de tiempo en cada instante y que son modificadas cada cierto tramo de tiempo. Cuando un usuario solicita el acceso a un sistema, el servidor le pide la clave que está vigente en ese tramo de tiempo, y el usuario mediante un dispositivo especial genera dicha clave. Es necesario que exista una sincronización entre los relojes internos de los dispositivos de los usuarios y de los servidores.

Este método es el más utilizado como mecanismo de autenticación dinámica para el acceso a los servidores de acceso remoto de múltiples organizaciones por parte de teletrabajadores. La Figura 17 muestra dos de los dispositivos comerciales de usuario más populares:

Figura 17: Dispositivos de usuario para autenticación mediante claves dependientes del tiempo

4.3.3 Claves basadas en reto

Otro mecanismo que se utiliza en los servicios y protocolos de acceso actuales es el uso de retos y respuestas en sustitución de la clave. En estos mecanismos, la clave no es dinámica, es decir, se mantiene la misma clave como secreto compartido entre el usuario y el sistema, no cambia. Sin embargo, no se solicita ni se envía la propia clave por la red en ningún momento, sino que el sistema al que se quiere acceder genera una pareja reto/respuesta, en el que la respuesta es función del reto y de la clave secreta compartida entre ambos. El cliente deberá resolver el reto y calcular la respuesta para poder acceder al servicio. El proceso se puede ver en la Figura 18.

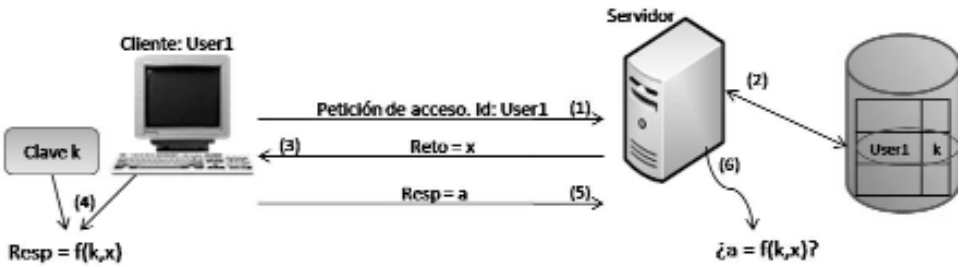

Figura 18: Sistemas reto/respuesta. Autenticación dinámica

Los pasos son los siguientes:

- El cliente remoto solicita acceso al sistema.
- El sistema genera una pareja reto/respuesta en el que la respuesta es función del reto y de la clave secreta. Resp = f(Reto, Clave).
- El sistema envía el reto al cliente.
- El cliente calcula la respuesta al reto que le han enviado en función de dicho reto y de la clave secreta compartida que él conoce.
- El cliente envía la respuesta al sistema.
- El sistema verifica que la respuesta recibida es correcta, y en función de ello, concede o deniega el acceso al servicio.

En este sistema, un atacante que esté monitorizando la red puede acceder al reto enviado, pero a partir de esta información no puede averiguar la respuesta dado que desconoce la clave necesaria para calcularla. Es más, aunque el atacante sea capaz de monitorizar múltiples parejas de retos/respuestas que se envían entre un cliente y un sistema remoto, será incapaz de obtener información útil, ya que el sistema remoto nunca va a enviar el mismo reto dos veces, y por otra parte, al estar la respuesta basada en una función de un solo sentido, sin inversa, es imposible obtener la clave a partir de múltiples retos y sus respuestas asociadas.

Este mecanismo es utilizado en múltiples sistemas de autenticación actualmente. El principal inconveniente del sistema radica en la necesidad de que el usuario debe realizar un cálculo complejo con el reto y su clave para calcular la respuesta. Este cálculo podría realizarse como en los métodos anteriores mediante un dispositivo externo, pero en los métodos de autenticación actuales, este cálculo lo realiza el propio cliente por software. Esto hace que este método sea resistente a la interceptación de la clave en la red, pero es vulnerable a la utilización de terminales no seguros, ya que es necesario introducir la clave real en el terminal para que pueda calcular la respuesta al reto recibido. Este tipo de autenticación se utiliza en el protocolo CHAP (*Challenge Authentication protocol*), utilizado por diversos mecanismos de acceso a redes y servicios.

4.3.4 Otros mecanismos

Existen modificaciones de los sistemas anteriores que permiten utilizarlos de manera más simplificada en entornos reales. Los más significativos son:

- Retos simplificados: se trata de sistemas reto/respuesta en los que la respuesta no se realiza por software sino que la calcula el propio usuario. Por ello, es necesario que el método de cálculo de respuestas al reto sea simple. Uno de los sistemas de este tipo más extendidos es la utilización de tarjetas de coordenadas, que el usuario posee, en el que el reto es una posición de dicha tarjeta y la respuesta el valor que existe en dicha posición. Este sistema tiene el inconveniente de que el número de retos posibles está limitado al número de posiciones de la tarjeta de coordenadas, por lo que es muy probable que se repita el mismo reto dos veces con el riesgo que esto conlleva en caso de que un atacante haya monitorizado previamente todos los retos de la tarjeta de coordenadas y sus respuestas asociadas.

- Uso de telefonía móvil: uno de los principales inconvenientes en los sistemas de autenticación dinámica es el hecho de que el usuario

tiene que transportar un dispositivo para el cálculo de la clave. Pero en la actualidad, y dado que prácticamente todos los usuarios disponen de un teléfono móvil, otra posibilidad es proporcionar la clave dinámica directamente a través de la red de telefonía móvil, a través de un mensaje corto o mensaje corto instantáneo. En este caso, el sistema remoto conocerá el número de teléfono móvil del usuario, y cada vez que el usuario realice un acceso al sistema remoto, le enviará mediante un mensaje corto la clave dinámica que el usuario debe utilizar para ese acceso. El usuario leerá la clave en su teléfono móvil y la introducirá en el cliente. Este sistema es resistente a la interceptación en red, ya que no se envía la clave real por la red, y a los terminales ajenos inseguros, ya que son claves de un solo uso. Además, el problema del dispositivo de cálculo de clave existente en los mecanismos anteriores desaparece, puesto que el usuario ya dispone de un teléfono móvil. El principal inconveniente de este sistema es el coste asociado a la utilización de redes de telefonía móvil para la transmisión de claves dinámicas.

4.4 Sistemas de gestión centralizada de autenticación

Una vez descritos los principales mecanismos de autenticación, sus debilidades y los métodos existentes para protegerse frente a dichas debilidades, es necesario analizar aspectos de implantación práctica de dichos sistemas de autenticación. Uno de los aspectos más importantes a tener en cuenta es la escalabilidad, ya que actualmente existen gran cantidad de sistemas remotos que ofrecen servicios a los que es necesario realizar una autenticación. Todos los sistemas remotos que ofrecen servicios quieren almacenar las claves de todos los usuarios que acceden al sistema por motivos de seguridad, por lo que será necesario que en todos estos sistemas el usuario haya realizado un registro previo de sus credenciales. Cada una de las credenciales de estos usuarios se guarda en el servidor remoto correspondiente. Esto da lugar a situaciones comprometidas ya que, por una parte, es una práctica adecuada mantener distintas claves en distintos servicios, para que si se compromete una clave en un servicio no se comprometa el resto de servicios en los que el usuario tiene registrada su clave, pero por otra parte, los usuarios no pueden en la práctica aprenderse distintas claves para cada servicio que utilicen, por lo que típicamente mantienen un conjunto reducido de claves que comparten entre distintos servicios, con los riesgos que esto conlleva.

La principal causa que provoca la anterior situación reside en la dualidad de funciones que asumen los servidores, ya que por un lado son servidores que dan un determinado servicio, y por otro son verificadores de las

credenciales de los usuarios cuya función es autenticarlos. Una proliferación de servicios utilizados por los usuarios, implicará una proliferación de verificadores y el problema ya relatado de multiplicidad de claves registradas.

La solución a este problema pasa por romper la dualidad de funciones que actualmente tienen los servidores. Por un lado existirán los servidores, que se encargarán únicamente de proporcionar un determinado servicio, y por otro lado el verificador, un servidor especial que se encargará de verificar las credenciales de los usuarios. Entre servidores y verificadores se establecen mecanismos de comunicación y cooperación permanentemente. Además, se puede disminuir el número de verificadores si múltiples servidores cooperan con un único verificador. En caso de que se tenga un solo verificador, se denominan sistemas de "Único Punto de Registro" (*Single Sign On* - SSO).

De esta forma, al romper la dualidad de funciones de los servidores, los usuarios sólo tienen que registrar sus claves en el verificador y éstas serán válidas para todos los servicios que ofrezcan los servidores que cooperen con ese verificador, permitiendo al usuario mantener una única clave, registrada en un solo sitio. Así se soluciona el problema de multiplicidad y repetición de claves.

El siguiente aspecto a abordar es definir el mecanismo de cooperación, es decir, cómo pueden cooperar los servidores y el verificador para que, por un lado, se verifiquen las credenciales del usuario correctamente, y por otra parte, los servidores puedan comprobar que el usuario ha sido verificado previamente con éxito en el verificador. Existen dos arquitecturas principales de cooperación entre servidores y verificador, como se ve en la Figura 19:

- Acceso indirecto a verificador. El usuario accede directamente al servidor que proporciona el servicio, y éste contacta con el verificador.

- Acceso directo a verificador. El usuario accede en primer lugar al verificador, y posteriormente accede al servidor que proporciona el servicio.

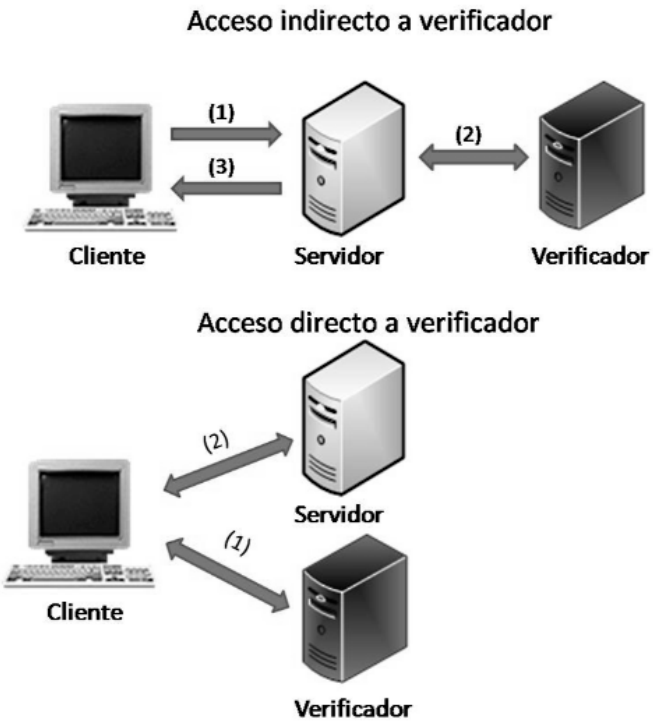

Figura 19: Acceso indirecto a verificador vs acceso directo

4.4.1 Acceso indirecto a verificador

Esta arquitectura presenta la gran ventaja de que el hecho de que exista un verificador separado del servidor (servidor y verificador son máquinas independientes) es algo transparente para el usuario. No es necesario modificar nada en ningún cliente ni proceso para utilizar el servidor configurado de esta forma, ya que las aplicaciones que se usaban con los servidores con autenticación local son perfectamente válidas. El usuario interactuará con el servidor de la misma manera que lo realizaba normalmente, pero existirá un proceso en el que las credenciales que el usuario proporcione al servidor son reenviadas desde el servidor al verificador para su comprobación. Este mecanismo de cooperación puede verse en la Figura 20, donde se observa que el usuario accede a dos servicios distintos proporcionados por servidores diferentes, pero la autenticación se realiza contra un mismo verificador. Además, la clave utilizada en ambos casos es la misma.

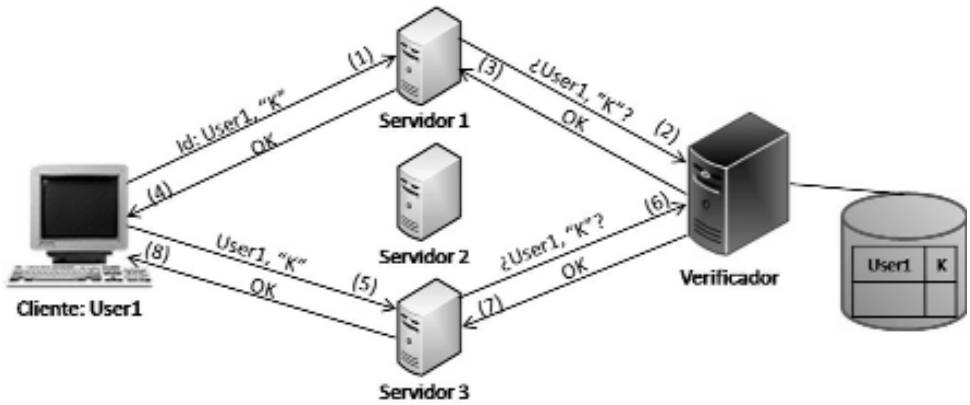

Figura 20: Autenticación con acceso indirecto a verificador

El principal problema que tiene esta arquitectura es que se proporciona información sensible a alguien que no la necesita, el servidor. Éste únicamente recoge las credenciales que le envía el usuario y las redirige al verificador, sin procesar en ningún momento las credenciales del usuario, ya que no es información que el servidor necesite. Pero el hecho de enviar las claves por sitios no seguros sin que sea necesario, genera un riesgo desde el punto de vista de la seguridad del sistema, ya que el servidor podría ser atacado o falsificado, y obtener la información sensible enviada por el usuario.

4.4.2 Acceso directo a verificador

En esta arquitectura, el usuario contactará primero con el verificador proporcionándole sus credenciales. El verificador comprobará la información recibida y si es correcta, le proporcionará una prueba de verificación ("Token") al usuario que éste deberá presentar a los servidores como prueba de que el usuario ha sido verificado previamente. Este mecanismo de cooperación puede verse en la Figura 21:

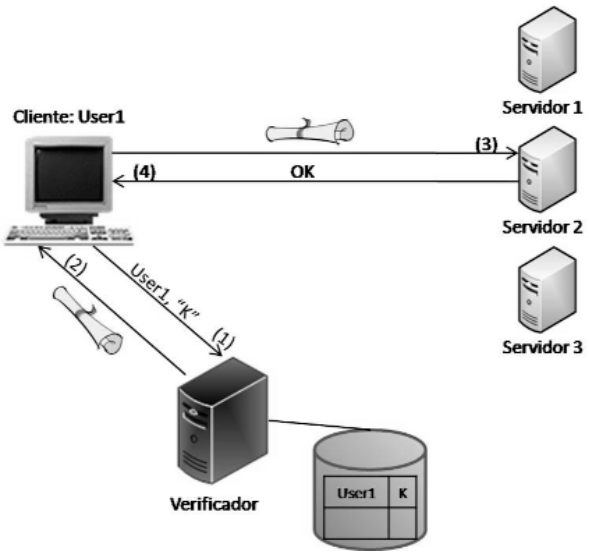

Figura 21: Autenticación con acceso directo a verificador

Las ventajas e inconvenientes de este sistema se complementan con la arquitectura anterior. Por un lado, la información sensible sólo es tratada por quien la necesita verdaderamente, el verificador, sin que transcurra por sistemas que no la necesitan. Sin embargo, esta arquitectura presenta un método de autenticación distinto al realizado tradicionalmente por las aplicaciones (acceso directo al servidor), por lo que las aplicaciones de los clientes y los servidores deben estar preparadas para realizar este tipo de autenticación. Es decir, no valen las aplicaciones tradicionales, sino que se tendrán que utilizar aplicaciones especiales que soporten este tipo de autenticación.

El acceso indirecto es mejor desde el punto de vista de la usabilidad y transparencia. Por el contrario, el acceso directo posee mayores prestaciones desde el punto de vista de la seguridad.

En las siguientes secciones se detallan los dos sistemas más representativos de cada una de las arquitecturas, KERBEROS y SAML, como arquitectura de acceso directo a verificador, y las arquitecturas AAA de acceso indirecto a verificador.

4.4.3 Kerberos

Se trata de una arquitectura de acceso directo al verificador que fue diseñada por el MIT en 1988, y que posteriormente ha sido revisada ligeramente. Es soportada hoy en día en múltiples aplicaciones y sistemas operativos, incluyendo Windows y Linux [17].

Esta arquitectura proporciona la verificación centralizada de usuarios, pero también de los servidores, incluyendo asimismo la provisión de claves de sesión para que puedan ser utilizadas en la fase de servicio. Se trata de una arquitectura de autenticación centralizada muy potente y segura, pero también compleja y que puede provocar retardos en los accesos a los servicios, por lo que su utilización se recomienda sobre todo en entornos corporativos en los que existe una red de comunicaciones rápida entre los usuarios y los servicios, pero no se recomienda su uso en un entorno extendido como es Internet.

En Kerberos existen dos verificadores principales:

- *Authentication Server* (AS), que almacena y gestiona las claves de los usuarios.

- *Ticket Granting Server* (TGS), que almacena y maneja las claves de los servidores.

El hecho de tener dos verificadores distintos va a proporcionar importantes ventajas a la hora de realizar una federación de dominios en la que los usuarios pueden utilizar servicios de otros dominios, como se verá más adelante. El esquema básico de Kerberos se muestra en la Figura 22 y es el siguiente:

1. El usuario se identifica ante el AS y éste le proporciona un ticket de sesión.

2. El usuario contacta con el TGS, identificándose con el ticket de la sesión anterior, para solicitar acceso a un servicio. El TGS verifica al usuario y le proporciona un ticket específico del servicio solicitado.

3. El usuario contacta con el servidor, proporcionándole el ticket de servicio anterior. El servidor comprueba el ticket y, si es correcto, comienza la fase de provisión de servicio.

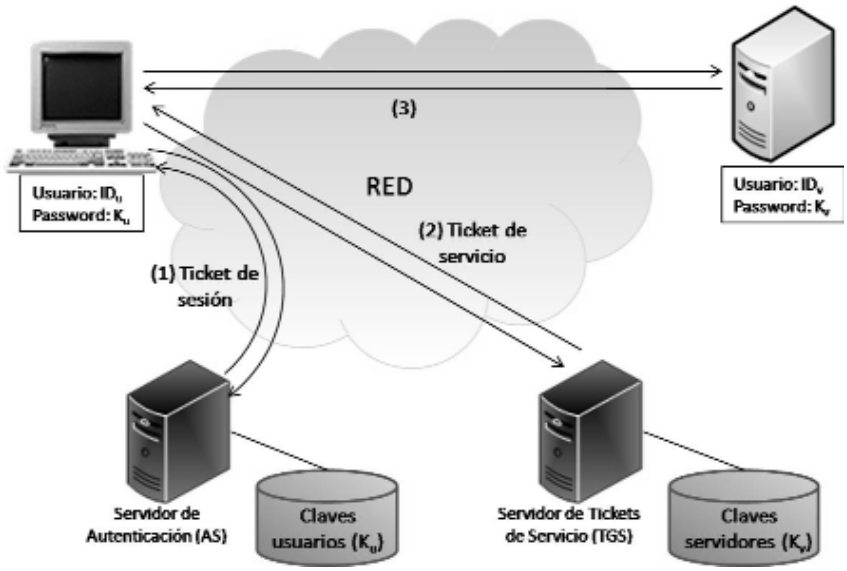

Figura 22: Arquitectura Kerberos

Como se observa en la Figura 22, Kerberos funciona con dos tipos de tickets generados por los verificadores. En primer lugar el usuario "inicia sesión" en el sistema, identificándose ante el AS. Esta "sesión" se materializa en un ticket de sesión que se proporciona al usuario y que tiene un tiempo de validez limitado, normalmente similar al tiempo que puede durar una sesión en el sistema (por ejemplo, una jornada de trabajo). De esta manera, el usuario sólo tiene que introducir sus credenciales cuando se conecta al sistema por primera vez en la jornada de trabajo (o durante el tiempo equivalente a la duración del ticket de sesión proporcionado), y no tiene que volver a introducirlas nuevamente. Todas las interacciones posteriores se realizan con el mismo ticket de sesión. Sólo si el usuario excede el tiempo de validez del ticket de sesión, éste quedará invalidado y será necesario generar uno nuevo contactando con el AS, para lo que deberá volver a introducir sus credenciales.

El ticket de sesión, sin embargo, sólo verifica que el usuario está autorizado a realizar una sesión en el sistema y que ha sido identificado correctamente, pero no da acceso a ninguno de los servicios de la organización. Para acceder a los servicios, el usuario deberá solicitar al segundo verificador (el TGS) un ticket del servicio específico al que quiere acceder. El TGS comprobará que el usuario está autorizado a utilizar dicho servicio y en caso afirmativo, generará un ticket de servicio que será proporcionado al usuario. Este ticket tiene un tiempo de validez limitado para la utilización del servicio, normalmente más reducido que el tiempo de validez de un ticket de sesión. En caso de que este tiempo sea excedido y el usuario quiera continuar accediendo al servicio, se volverá a solicitar al TGS, de una forma transparente para el usuario, un nuevo ticket de servicio siempre que el ticket de sesión del usuario siga siendo válido.

Un aspecto fundamental en las arquitecturas de acceso directo al verificador es la seguridad de las pruebas (los "tokens") que el verificador proporciona al usuario para que éste lo transmita a los servicios. En el caso de Kerberos, se trata de la seguridad de los tickets de sesión y de servicio. En caso de que un ticket pudiera ser falsificado, el sistema podría ser atacado fácilmente, de forma que los tickets tienen que tener la protección adecuada para que no puedan ser falsificados por atacantes. Esta protección se consigue cifrando los tickets con la clave de quien los tiene que comprobar, es decir, los ticket de sesión se usan para solicitar al TGS tickets de servicio, por lo que se cifran con la clave del TGS. De igual manera, los tickets de servicio deben ser comprobados por los servidores, por lo que se cifran con las claves de los servidores, de forma que un atacante que no conozca las claves no podrá falsificar el ticket ni descifrarlo para modificarlo.

A continuación se explican con detalle las tres interacciones básicas en Kerberos. Debe notarse que el detalle proporcionado es el correspondiente a la versión 4 de Kerberos. Posteriormente el MIT ha generado la versión 5 que soluciona algunos problemas de seguridad y escalabilidad, y es la que se utiliza actualmente. Pero desde un punto de vista de comprensión del funcionamiento de Kerberos, se ha considerado conveniente explicar la versión 4 ya que resulta más sencilla de comprender, explicando posteriormente las principales diferencias existentes entre ambas versiones.

4.4.3.1 Fases de Kerberos

Fase 1: Acceso al AS

En esta fase, el usuario accede al *Authentication Server* para solicitar un ticket de sesión. Para mejorar la seguridad, la autenticación se realiza de forma indirecta, es decir, el usuario sólo transmite su identidad, no sus credenciales, y el AS le responde con un mensaje cifrado con su clave de usuario. Si el usuario sabe descifrar el mensaje, tendrá acceso al ticket de sesión que ha sido generado y podrá seguir utilizando el sistema. Este proceso puede verse en la Figura 23:

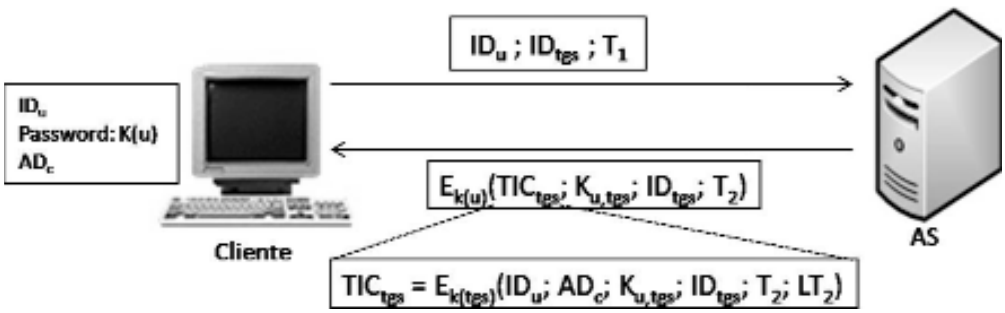

Figura 23: Fase 1 de Kerberos: Acceso al AS

En las interacciones de la figura se muestran los siguientes parámetros:

- ID_u: Identificador del usuario.
- ID_{tgs}: Identificador del TGS al que va a solicitar tickets de servicio.
- TIC_{tgs}: Ticket de sesión.
- $K_{u,tgs}$: Clave de sesión generada por el AS para la comunicación del usuario con el TGS.
- T_i: Instante de tiempo del mensaje i.
- LT_2: Tiempo de vida (*Lifetime*) del ticket de sesión.
- $K_{(tgs)}$: Clave del TGS.
- K(u): Clave del usuario u.
- AD_c: Dirección desde la que se conecta el usuario u.

Cuando el usuario quiere acceder a un servicio, en primer lugar debe contactar con el AS. Como se ve en la figura, el usuario sólo se identifica mediante su identificador, proporcionando asimismo el identificador del TGS al que va a solicitar tickets de servicios, es decir, el identificador del dominio que va a utilizar, para abrir sesión en dicho dominio. El *Authentication Server*, que conoce las claves de los usuarios, le contesta con un mensaje cifrado con la clave del usuario ($E_{K(U)}$), de manera que se consigue una autenticación indirecta, y sólo si el usuario conoce la clave podrá descifrar el mensaje y acceder a su contenido, obteniendo el ticket de sesión que le permitirá continuar con el proceso. El ticket de sesión está incluido dentro del mensaje cifrado enviado desde el AS al usuario.

Si se analiza el contenido del mensaje devuelto por el AS, se observa que aparte de datos de tiempo y de identificación del TGS, el AS proporciona al usuario un ticket de sesión y una clave de sesión para que sean utilizados posteriormente en las interacciones entre el usuario y el TGS. Esta clave de sesión aleatoria la genera el AS para que sea utilizada entre el usuario y el TGS, y se la proporciona al usuario en dicho mensaje. Esta clave, además de al usuario, también se le proporciona al TGS, pero no directamente, sino indirectamente dentro del ticket de sesión.

El ticket de sesión es un conjunto de datos cifrados con la clave del TGS, que el AS debe conocer. Estos datos incluyen los datos del usuario (su identificador y su dirección), así como la hora de generación del ticket y su tiempo de vida, aparte de contener también la clave que el AS generó para la comunicación entre el usuario y el TGS. El usuario recogerá este ticket de sesión y lo guardará para poder solicitar tickets de servicio mientras sea válido, pero al estar cifrado con la clave del TGS no podrá acceder a su contenido.

Fase 2: Acceso al TGS

En esta fase, el usuario, que tiene un ticket de sesión válido, accede al TGS para solicitar un ticket de servicio para el servicio "v". El intercambio de mensajes que se produce, se puede ver en la Figura 24:

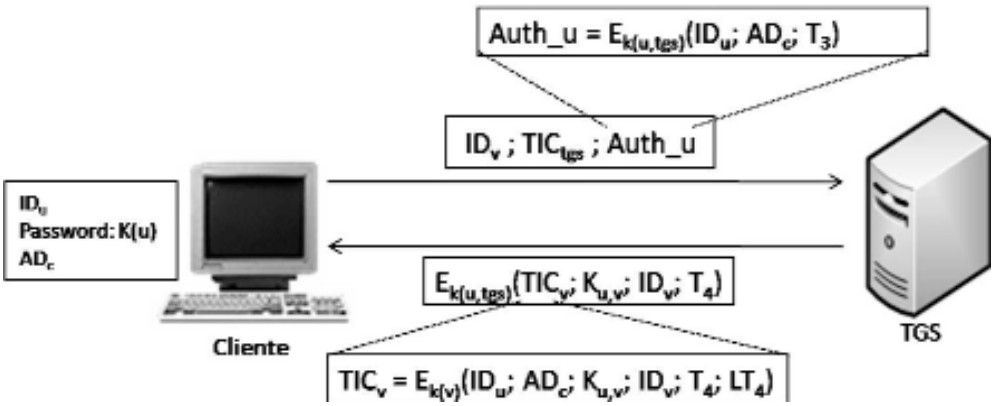

Figura 24: Fase 2 de Kerberos. Acceso al TGS

En dicha figura, el significado de los parámetros es el siguiente:

- ID_V: Identificador del servidor que proporciona el servicio solicitado.
- TIC_{TGS}: Ticket de sesión.
- $Auth\_u$: Autenticador del usuario u.
- $K_{U,TGS}$: Clave de sesión generada por el AS para la comunicación del usuario con el TGS.
- ID_U: Identificador del usuario.
- AD_C: Dirección desde la que se conecta el usuario u.
- TIC_V: Ticket del servicio v.
- $K_{U,V}$: Clave de sesión generada por el TGS para la comunicación del usuario con el servidor que proporciona servicio v.

- T_i: Instante de tiempo del mensaje i.

- LT_4: Tiempo de vida (*Lifetime*) del ticket de servicio.

Como se puede ver en la figura, el usuario solicita al TGS un ticket de servicio proporcionando el identificador del servidor que proporciona el servicio solicitado, el ticket de sesión que le fue dado en la fase anterior, y un autenticador en el que cifra sus datos personales (identificador/dirección) con la clave de sesión $K_{U,TGS}$, que se usa para las comunicaciones entre el usuario u y el TGS.

EL TGS al recibir estos parámetros, lo primero que hace es descifrar el ticket de sesión (que fue cifrado con la clave del TGS) y extraer la información que éste contiene, los datos del usuario y la clave de sesión que el AS generó, $K_{U,TGS}$. Con esta clave, el TGS puede descifrar el autenticador y comprobar que los datos del usuario incluidos en el autenticador coinciden con los datos del ticket de sesión, autenticando de esta manera al usuario que ha solicitado el ticket de servicio.

En este momento, el TGS comprueba si el usuario está autorizado a utilizar el servicio "v", y si es así genera un ticket del servicio "v" y se lo envía al usuario. Al igual que el AS en la fase anterior, el TGS genera una clave de sesión para que el usuario u y el servidor que proporciona el servicio solicitado puedan comunicarse. El TGS envía al usuario un mensaje que contiene el ticket de servicio generado, la clave de sesión, el identificador del servidor y datos relacionados con el tiempo de generación del mensaje. Este mensaje está cifrado con la clave de sesión que comparten el usuario y el TGS, conocida por el usuario.

El ticket de servicio que genera el TGS sigue una estrategia similar al ticket de sesión de la fase anterior. Se trata de un ticket cifrado con la clave del servidor que proporciona el servicio (el TGS almacena las claves de los servidores) en el que se incluyen los datos del usuario y la clave de sesión que el TGS ha generado para la comunicación entre el usuario y el servidor.

Fase 3: Acceso al servidor

En esta última fase, el usuario accede al servidor del servicio directamente presentándole el ticket de servicio que le fue entregado en la fase anterior, así como un autenticador en el que cifra sus datos personales con la clave de sesión entre el usuario y el servidor que le fue entregada anteriormente. La Figura 25 muestra el proceso correspondiente a esta fase:

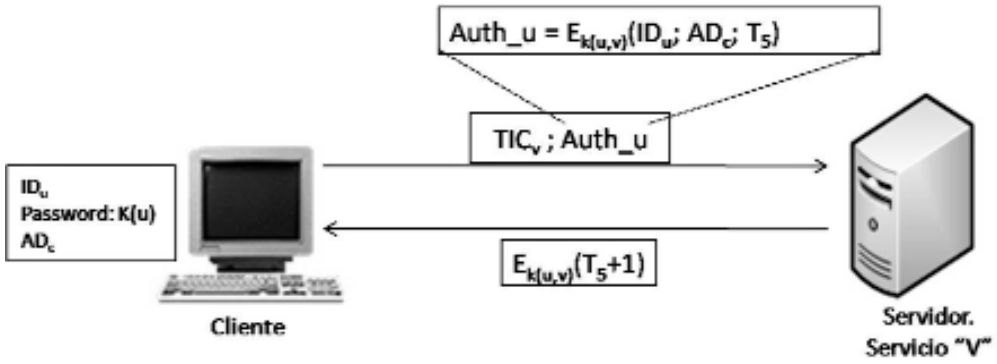

Figura 25: Fase 3 de Kerberos. Acceso al servidor

Los parámetros intercambiados en esta fase son:

- TIC_V: Ticket de servicio.
- $Auth_{\_u}$: Autenticador del usuario u.
- ID_U: Identificador del usuario.
- AD_C: Dirección desde la que se conecta el usuario u.
- $K_{U,V}$: Clave de sesión generada por el TGS para la comunicación del usuario con el servidor del servicio "v".
- T_i: Instante de tiempo del mensaje i.

El servidor al recibir el ticket de servicio y el autenticador, lo primero que hace es descifrar el ticket con la clave del servidor. Este hecho permite llevar a cabo, indirectamente, la autenticación del servidor, ya que si el servidor fuera falso, no podría descifrar el ticket de servicio ni continuar el proceso. Al descifrar el ticket, el servidor obtendrá los datos personales del usuario y la clave de sesión que fue generada anteriormente por el TGS. Una vez en posesión de estos datos, el servidor usará esa clave de sesión para descifrar el autenticador recibido, y verificar que los datos de usuario que contiene coinciden con los del ticket de servicio, probando de esta manera la autenticidad del usuario y de la petición. Por último, el servidor envía al usuario un mensaje de confirmación consistente en la hora de la petición anterior más uno, cifrado con la clave de sesión $K_{U,V}$, que ambos comparten. Tras el envío de ese mensaje, el usuario y el servidor pasan a la fase de provisión del servicio, en la que pueden utilizar de forma opcional esa clave de sesión para proteger los mensajes intercambiados.

4.4.3.2 Kerberos versión 5

Como ya se dijo anteriormente, tras la versión 4 original se ha desarrollado la versión 5 de Kerberos, que no modifica la estructura esencial del proceso, sino que añade pequeñas mejoras y solución de deficiencias identificadas. Las más significativas son:

- Se evita la utilización de doble cifrado que se realiza en la versión 4. Los tickets no se envían cifrados por las claves de sesión.

- Se permite la utilización de distintos formatos de direcciones de red, permitiendo así su utilización por protocolos distintos a IPv4.

- La codificación de mensajes se realiza con ASN.1 de acuerdo a los estándares.

- Se permite la utilización de distintos algoritmos de cifrado. La versión 4 imponía la utilización de DES como algoritmo de cifrado.

4.4.3.3 Federación de dominios en Kerberos

Kerberos puede ser utilizado para realizar una federación entre distintos dominios de una forma muy sencilla, al estar separados los verificadores de los usuarios (*Authentication Server*) y de servidores (*Ticket Granting Server*). Si existe un acuerdo entre dos dominios distintos en los cuales se dispone de una infraestructura Kerberos en cada una de ellos, el usuario de un dominio puede solicitar la utilización de un servicio del otro dominio, tal y como se presenta en la Figura 26:

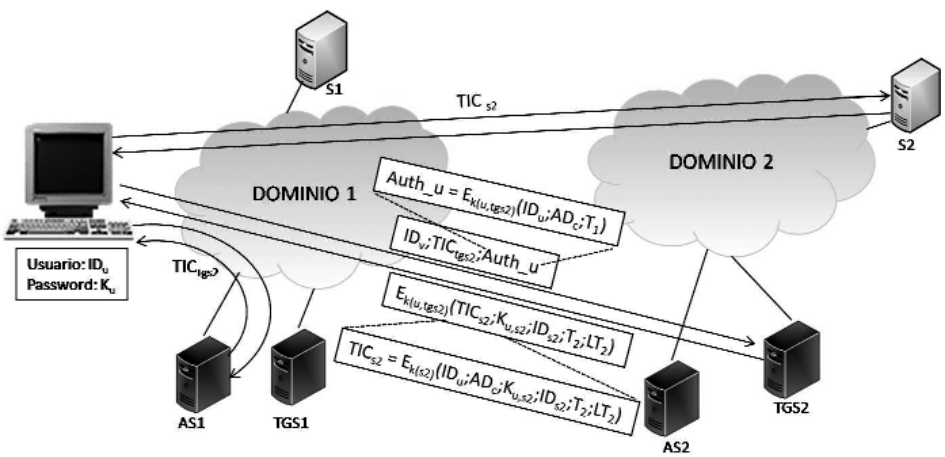

Figura 26: Federación de dominios en Kerberos

El acuerdo entre los dominios implica que los *Authentication Server* de cada uno de los dominios pueden emitir tickets de sesión utilizables en el otro dominio, lo cual implica que cada AS tiene la clave del TGS del otro dominio.

De esta manera, el usuario en la fase 1 mandará sus datos de identificación al AS de su dominio (Dominio 1), pero con el identificador del TGS del otro dominio, solicitando así iniciar la sesión en el Dominio 2. El AS comprobará la autorización y le enviará un ticket de sesión del Dominio 2 cifrado con su clave de usuario. El usuario descifrará el mensaje que contiene el ticket de sesión y se comunicará directamente con el TGS del Dominio 2 para solicitar un ticket de servicio del servidor que quiere utilizar en el Dominio 2. Como el ticket de sesión está cifrado con la clave del TGS del Dominio 2, éste podrá descifrarlo y emitir el correspondiente ticket de servicio del servidor solicitado.

De esta manera puede realizarse una federación entre dominios sin tener que ceder las claves de los usuarios o de los servicios a otros verificadores de dominios distintos.

4.4.4 SAML

Kerberos tiene una arquitectura de acceso directo a verificador muy robusta y escalable, pero a la vez muy compleja, lo cual hace que su uso se restrinja a entornos corporativos en los que se dispone de comunicaciones rápidas y fiables y no existan grandes retardos en la red. Pero este sistema no escala adecuadamente para su utilización en entornos extendidos, como puede ser el acceso a servicios a través de Internet.

La solución más madura de las que se han propuesto para su uso en el acceso a servicios a través de redes extensas es el protocolo SAML, para su utilización sobre todo en entornos de acceso a Servicios Web (Web Services) [18].

SAML (*Security Assertion Markup Language*) es un estándar XML para intercambio de datos de autenticación y autorización entre entidades. De esta manera, un cliente enviará una solicitud de autenticación o autorización a un Proveedor de Identidad (IdP - *Identity Provider*), y éste, tras comprobar la autenticación o autorización solicitada, le responderá con un mensaje que contiene un aserto confirmando la certeza de la autenticación o autorización solicitada. Este aserto será posteriormente facilitado a distintos servicios para que éstos puedan validarlo y así verificar indirectamente la autenticación o autorización del cliente. Para ello, es necesario

que estos asertos estén suficientemente protegidos de manera que se evite una manipulación o falsificación de ellos por parte de clientes maliciosos. Podría considerarse que SAML mantiene la filosofía de "tokens" de Kerberos, pero aplicado a Servicios Web.

SAML es utilizado sobre todo en entornos extendidos de Servicios Web que manejan mensajes codificados en formato XML.

4.4.5 Arquitecturas AAA

Bajo este nombre se engloban las arquitecturas de acceso indirecto al verificador, en el que el verificador se encuentra detrás del servidor, y el usuario no accede directamente a él (ver Figura 20). Estas arquitecturas presentan una gran ventaja y un gran inconveniente en comparación con las arquitecturas de acceso directo al verificador:

- La ventaja principal es que el hecho de que el cliente no tenga que interactuar con el verificador hace que su existencia no sea visible para el cliente, es decir, que la existencia del verificador es transparente al usuario. Por tanto, el usuario interactuará con los servidores de la misma manera que lo haría en caso de que no existiera un verificador. Esto permite utilizar las mismas aplicaciones clientes tradicionales que existen en entornos sin sistemas de autenticación centralizada, sin necesidad de aplicaciones específicas adaptadas para su utilización en estos entornos, como es el caso de los sistemas de acceso directo a verificador como Kerberos o SAML.

- Pero por otro lado, tienen el inconveniente de que se transmite información sensible de seguridad a través de entidades que no la necesitan, que simplemente hacen de pasarelas para este tipo de información. En efecto, el papel de los servidores en esta arquitectura durante la fase de autenticación se reduce a recoger la información de autenticación enviada por los clientes y retransmitirla al verificador, por lo que se está enviando a los servidores información de autenticación que no necesitan. En principio, esto no debería ser un problema, sin embargo este hecho aumenta los riesgos ante amenazas de suplantación de los servidores por servidores maliciosos, que obtendrían de forma directa la información de autenticación de los usuarios.

El nombre AAA proviene de las iniciales de "*Authentication, Authorization and Accounting*", que reflejan la funcionalidad de los verificadores en esta arquitectura [19]:

- Autenticación: esta arquitectura proporciona un sistema de autenticación centralizada y punto único de registro (*Single Sign On*) de credenciales.

- Autorización: esta arquitectura proporciona al servidor, además del resultado de la autenticación, información sobre las características de autorización del usuario, con diversos datos sobre el usuario que el servidor podrá procesar y gestionar de forma adecuada, usualmente para aplicar distintas políticas de autorización del usuario, pero que puede ser utilizado para otros objetivos.

- Contabilidad: esta arquitectura proporciona contabilidad a los servidores, de forma que el verificador puede mantener el registro de los accesos al servicio y diversos datos que permitan posteriormente aplicar una política de contabilidad.

El ámbito de las arquitecturas AAA se circunscribe a la comunicación entre el servidor y el verificador, estableciendo el protocolo de comunicación entre ambos y el formato y sintaxis de la información transmitida. La arquitectura AAA no establece ningún tipo de restricción acerca de la comunicación entre el cliente y el servidor. De hecho, el protocolo de la arquitectura AAA debe poder utilizarse con cualquier tipo de protocolo de comunicación entre el cliente y el servidor que incluya una fase de autenticación. El protocolo AAA se establece precisamente en esa fase de acceso entre la solicitud de autenticación del cliente y la respuesta desde el servidor, como puede verse en la Figura 27.

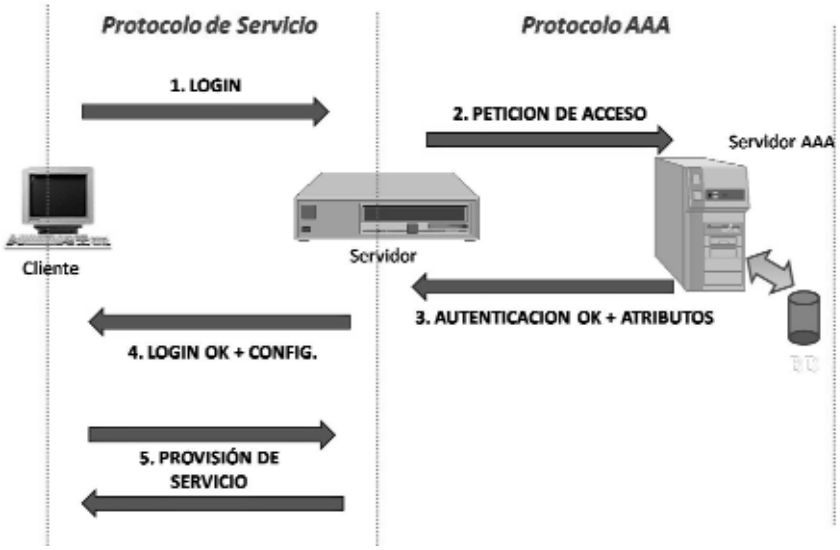

Figura 27: Modelo AAA

Los primeros exponentes de arquitecturas AAA surgieron como solución al problema del acceso a red proporcionado por los ISP (*Internet Service Provider*). Estas compañías ofrecían nodos de conexión (Puntos de Presencia o POP - *Point of Presence*) a lo largo de toda la geografía para que los usuarios utilizaran el más conveniente para ellos para acceder a la red. Sin embargo, esto requería la identificación del usuario cada vez que accedía a cualquiera de los nodos del proveedor, por lo que se hizo evidente la necesidad de un enfoque de autenticación centralizada, un único nodo que almacenara la información de autenticación de todos los usuarios, y que fuera accesible desde cualquiera de los nodos de acceso para verificar las credenciales proporcionadas por los usuarios.

Uno de los primeros protocolos utilizados con ese fin fue el protocolo TACACS (*Terminal Access Controller Access-Control System Plus*) de Cisco. Este protocolo fue rediseñado posteriormente bajo el nombre de TACACS+, que proporciona de una forma separada aspectos de autenticación y autorización. Sin embargo, estos protocolos son soluciones propietarias y la industria demandaba una solución estándar independiente del fabricante, por lo que en el IETF se diseñó y estandarizó el protocolo RADIUS, que proporciona la funcionalidad AAA demandada de una forma estándar.

4.4.5.1 RADIUS

El protocolo RADIUS (*Remote Authentication Dial-In User Server*) es un protocolo de tipo cliente-servidor que permite a distintos tipos de servidores interactuar con un servidor AAA para gestionar la autenticación, autorización y contabilidad de los accesos de los usuarios al servidor. Está definido en las RFC 2138 y 2139, y aunque originalmente estaba orientado a la interacción con servidores de acceso a red, actualmente se utiliza e interactúa con múltiples tipos de servidores.

El protocolo RADIUS se ejecuta entremezclado con la fase de login del protocolo de acceso al servicio, como se muestra en la figura anterior (Figura 27). Implementa las tres funcionalidades principales de las arquitecturas AAA:

- *Authentication*: cuando el servidor recibe la petición de *login* del usuario, reenvía los datos de credenciales del usuario y opcionalmente, información que se conoce del usuario, al servidor RADIUS mediante un mensaje ***Access-Request***. La transmisión de las credenciales del usuario en esta primitiva del protocolo RADIUS se realiza cifrada, independientemente de que fueran enviadas en claro o no en el protocolo de acceso. El servidor RADIUS comprobará las credenciales con la información registrada sobre el usuario, y responderá enviando una de las primitivas siguientes:

  - ***Access-Reject***: se rechaza la petición de acceso. Puede ser debido a credenciales incorrectas, autorizaciones inadecuadas, usuario inexistente, etc.

  - ***Access-Challenge***: la fase de login del protocolo de acceso no se realiza con la transmisión de credenciales del usuario, sino que se realiza mediante la técnica reto-respuesta. En este caso, el servidor RADIUS genera un reto que es enviado al servidor con el mensaje ***Access-Challenge***, para que éste lo reenvíe al usuario y pueda generar la respuesta adecuada, que será transmitida desde el servidor al servidor RADIUS con un nuevo mensaje ***Access-Request***. Este proceso puede verse en la Figura 28:

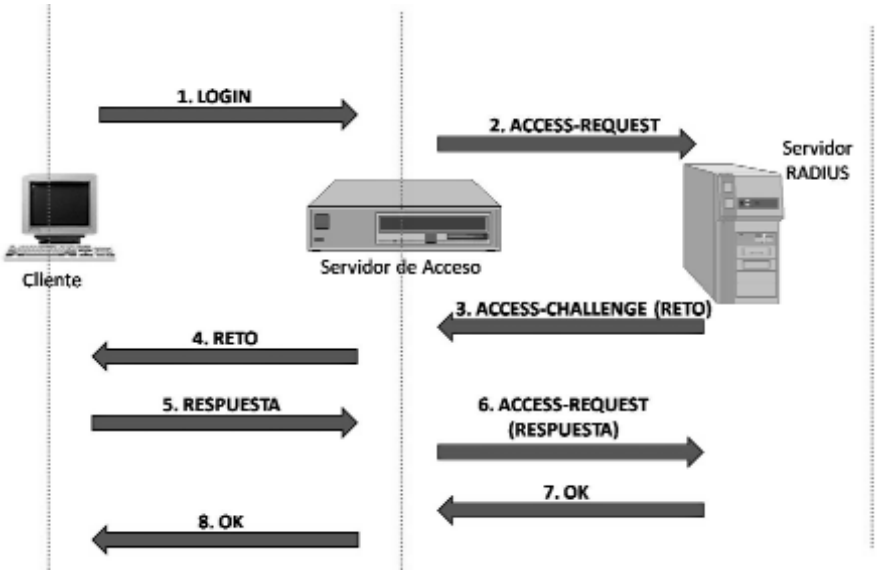

Figura 28: Autenticación basada en reto con RADIUS

- ***Access-Accept***: el usuario se ha identificado correctamente y se le garantiza el acceso al servicio con las autorizaciones pertinentes referidas al usuario.

- *Authorization*: el servidor RADIUS puede incluir información de autorización del usuario en la respuesta del mensaje ***Access-Accept***. Esta información será interpretada por el servidor de acceso de forma adecuada para garantizar las autorizaciones del usuario. Los atributos de autorización que se pueden transmitir en RADIUS son numerosos, incluyendo:

  - Dirección IP y máscara de subred que debe asignarse a un usuario.

  - Tipo de servicio que se le puede proporcionar a un usuario, por ejemplo, *Login* (conexión a sistema remoto), *Framed* (protocolo a iniciar con el usuario como por ejemplo PPP), etc.

  - *Framed-Protocol*, tipo de protocolo que se debe iniciar con el usuario.

  - Identificador de filtro para implementar listas de acceso por parte del servidor.

- Atributos específicos del tipo de servicio de *Login*.

- Parámetros relativos a calidad del servicio.

- Temporizadores de sesión o de inactividad.

- *Vendor-Specific*: atributos extendidos específicos de fabricantes o de escenarios.

- *Accounting*: el servidor puede solicitar al servidor RADIUS un mensaje ***Accounting-Request*** con el parámetro "*Start*" cuando un usuario ha sido autenticado y autorizado y comienza su sesión. Durante la sesión del usuario, el servidor puede enviar mensajes de ***Accounting-Request*** con el parámetro "*Interim Accounting*" para actualizar datos sobre la sesión del usuario. Finalmente, el servidor enviará el mensaje ***Accounting-Request*** con el parámetro "*Stop*", para finalizar el proceso de contabilidad, cuando la sesión del usuario finalice.

El protocolo RADIUS se utiliza en gran número de instalaciones para proporcionar y facilitar una solución de registro y autenticación centralizada, por lo que pueden existir problemas de escalabilidad cuando se aplica a un gran número de usuarios y servidores que acceden simultáneamente al servidor RADIUS. Para evitar estos problemas de escalabilidad, la arquitectura AAA basada en RADIUS puede basarse en una distribución de servidores RADIUS, en la que existirán servidores que ofrezcan el papel de "proxy RADIUS", encargados de direccionar la petición RADIUS al servidor más adecuado.

Asimismo, RADIUS se puede utilizar para el acceso a servicios de dominios externos, siempre y cuando exista un acuerdo entre el dominio origen y el dominio visitado. En este caso, al utilizarse una identificación basada en dominios ("*realms*"), del tipo usuario@dominio, el servidor RADIUS del dominio visitado puede ponerse en contacto con el servidor RADIUS del dominio origen para verificar la autenticación del usuario y conseguir los parámetros necesarios de autorización.

4.4.5.2 DIAMETER

El protocolo RADIUS ha tenido una gran aceptación y se utiliza ampliamente en múltiples entornos. Sin embargo, se trata de un protocolo que se diseñó sobre todo para escenarios de acceso a Internet por acceso telefónico con el protocolo PPP. El crecimiento actual de Internet y la introducción de nuevas tecnologías de acceso, como redes inalámbricas, DSL, IP Móvil o Ethernet, introducen nuevos requisitos a los protocolos AAA que RADIUS no puede proporcionar de forma nativa.

Por ello, se define el protocolo DIAMETER como sucesor de RADIUS, aunque ambos protocolos son incompatibles entre sí. El concepto clave de DIAMETER es la definición de un protocolo base, con funcionalidad similar a la de RADIUS, pero extensible de una forma estándar para adecuarse a determinados escenarios.

Las principales mejoras frente a RADIUS son:

- Usa una infraestructura de protocolos segura, como IPSEC o TLS.

- Usa un protocolo de transporte fiable, en vez de UDP.

- Soporta nativamente el uso de proxies, algo que en RADIUS se utilizaba de facto pero no estaba contemplado en el estándar.

- Permite negociación de capacidades, que permite conocer posibles extensiones de DIAMETER implementadas.

- Incluye mensajes enviados por el servidor para solicitar reautenticación o reautorización bajo demanda.

- Se mejora el soporte de *roaming*.

Sobre este protocolo base, se pueden definir extensiones conocidas como "Aplicaciones de DIAMETER". Estas aplicaciones pueden definir nuevos comandos y nuevos conjuntos atributo/valor. Ejemplos de extensiones definidas para DIAMETER son:

- *Mobile IPv4 Application.*

- *Network Access Server Application.*

- *Extensible Authentication Protocol Application.*

- *Credit Control Application.*

- *Session Initiation Protocol Application.*

Capítulo 5

Sistemas de defensa perimetral

5. Sistemas de defensa perimetral

Los sistemas de autenticación y autorización descritos en el capítulo anterior facilitan un control de acceso lógico a los servicios proporcionados a usuarios externos autorizados. El siguiente paso es proteger la infraestructura del resto de intentos de acceso a servicios que no deben ser utilizados por usuarios externos. Como se vio anteriormente, los intentos de acceso a estos servicios son una de las principales fuentes de ataques, al explotar vulnerabilidades software de los servidores.

Por ello, el principal mecanismo de defensa reside en lo que se conoce como "Defensa perimetral", un conjunto de filtros que restringen el acceso de las peticiones entrantes antes de que lleguen al servidor, es decir, en el perímetro de la infraestructura que se quiere proteger. El objetivo de la defensa perimetral no es otro que restringir el intento de accesos externos no permitidos a los servicios internos de la organización protegida [20].

Existen dos soluciones básicas de defensa perimetral, que dependen del alcance de la infraestructura protegida: la defensa perimetral de un sistema y la defensa perimetral de una subred.

5.1 Defensa perimetral de sistema

Las soluciones tecnológicas que permiten este tipo de defensa perimetral se denominan cortafuegos personales. Este método se basa en proteger un sistema individual de los intentos de ataque que le llegan por la red, actuando a la entrada de cada sistema vulnerable. Por ello, esta defensa debe establecer una interceptación de las peticiones antes de que lleguen a los servidores de la capa de aplicación y las intenten procesar. Dependiendo del nivel donde se lleva a cabo esta interceptación y filtrado de las peticiones entrantes, se pueden tener distintos tipos de sistemas:

- Interceptores TCP (TCP-*Wrappers*). Se trata de filtros que se ubican entre el nivel de transporte y el nivel de aplicación y que capturan la petición justo antes de ser atendida por el servidor.

- Interceptores de nivel de red. El filtro se ubica en el nivel de red.

En la Figura 29 se observa la ubicación dentro de la torre de protocolos de ambos tipos de interceptores:

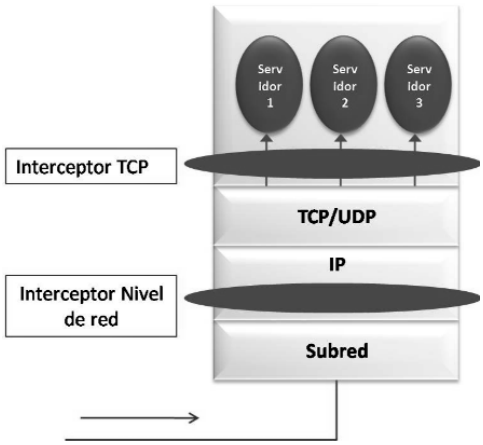

Figura 29: Cortafuegos personales con dos niveles de interceptores

5.1.1 Interceptores TCP

Este tipo de soluciones de defensa perimetral de sistema fue el primero que se desarrolló como mecanismo de protección de sistemas, ya que no exigía modificar el software de la torre de protocolos y se basaba en los denominados servidores dinámicos, que se arrancaban bajo demanda cuando había una petición para ellos. Estos sistemas, que se basaban en el sistema operativo UNIX, modificaban la secuencia de arranque del servidor de forma que se ejecutaba primero un filtro que comprobaba la petición entrante frente a un fichero de reglas, y si la petición era consentida, entonces se arrancaba el servidor.

Este sistema tenía muchos problemas que hacían que no fuera una solución adecuada:

- Sólo protegía los servicios que se arrancaban dinámicamente, pero no los servicios que se ejecutaban constantemente (modo "daemon"), los cuales no se veían afectados por las modificaciones de la secuencia de arranque.

- Sólo era válido para servicios basados en el protocolo TCP. Este modo de arranque dinámico de servidores no era válido para servicios basados en UDP, que al no estar orientados a conexión no podían ser arrancados bajo demanda para atender una conexión y parados cuando ésta acabase.

- No era válido para las conexiones salientes. Solo podía capturar conexiones entrantes.

5.1.2 Interceptores de nivel de red (Cortafuegos personales)

Con el propósito de solucionar los problemas que tenían los interceptores de nivel de transporte descritos anteriormente, surgieron los interceptores de nivel de red, también denominados cortafuegos personales. Este tipo de sistemas de defensa perimetral proporcionaba una solución completa al problema de la defensa perimetral de sistemas. La solución se basa en incluir el interceptor de tráfico en el nivel de red, junto al protocolo IP, como se observa en la Figura 29. De esta forma, todas las peticiones entrantes (y las salientes) deben atravesar el filtro, por lo que se corrige el principal problema de los interceptores TCP. Además, es válido para servicios basados tanto en TCP como en UDP, ya que captura el tráfico a nivel IP.

Sin embargo, tiene el inconveniente de que no es una tecnología tan sencilla de implantar como la anterior, ya que es necesario alterar el núcleo de la capa de red del sistema operativo. Las primeras soluciones de cortafuegos personales fueron productos independientes, aunque posteriormente los fabricantes de productos de seguridad las incluyeron como un producto más dentro de las suites de seguridad que proporcionaban los antivirus. Actualmente la tendencia es incluirlo como parte de los sistemas operativos, algo que en los sistemas operativos Windows comenzó en el *Service Pack 2* de Windows XP (Figura 30).

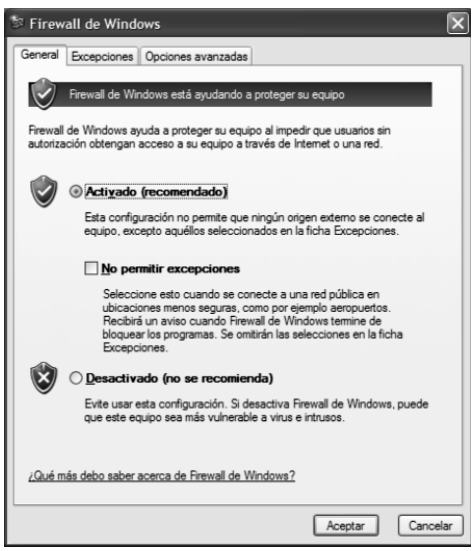

Figura 30: *Firewall* de Windows XP

Este tipo de cortafuegos personales funciona contrastando los datos de las peticiones entrantes o salientes frente a una definición de reglas de seguridad. Los datos suelen incluir la dirección IP origen y el servicio solicitado, permitiendo mayor o menor grado de granularidad para la definición de las reglas y de las acciones (típicamente aceptar o rechazar).

Un aspecto novedoso es la aplicación de los cortafuegos personales para el control de las peticiones salientes, pudiendo indicar las aplicaciones autorizadas a conectarse a Internet. De esta forma, se puede luchar contra los programas espía que se conectan a Internet sin autorización para el envío de datos personales.

5.2 Defensa perimetral de red

La solución de cortafuegos personales vista en la sección anterior es de utilidad en entornos pequeños, compuesto por uno o varios sistemas a proteger, en los que es posible configurar y administrar individualmente la protección perimetral de cada uno de los sistemas. Sin embargo, en un entorno más amplio, en el que el número de sistemas es elevado y están interconectados entre ellos con distintas subredes y equipos de interconexión, la complejidad de administración de los cortafuegos personales de cada uno de los equipos puede llegar a ser muy elevada, debido a tres factores principales:

- Multiplicidad de equipos. Una solución de cortafuegos personales sólo es viable desde un punto de vista de administración y mantenimiento cuando el número de sistemas a gestionar es pequeño. Cuando el volumen de sistemas a proteger aumenta, la complejidad de configurar y mantener las configuraciones de seguridad de los sistemas, así como de aplicar parches de seguridad, comprobar configuraciones deficientes de seguridad, etc., es demasiado alta y el riesgo de fallos de administración de seguridad puede aumentar peligrosamente.

- Heterogeneidad de equipos. En un entorno compuesto por múltiples sistemas, éstos pueden ser heterogéneos desde el punto de vista de su arquitectura hardware y software, con distintos sistemas operativos, diferentes configuraciones de servicios de red, etc. Esta heterogeneidad de los sistemas hace que la configuración de seguridad de cada uno de ellos sea una tarea específica y distinta, multiplicando la complejidad de la administración de seguridad del conjunto de sistemas individuales.

- Inclusión de equipos antiguos. En muchos entornos es necesaria la existencia de equipos con versiones antiguas e inseguras de sistemas

operativos o servidores de red, debido, entre otras razones, a la necesidad de ejecutar programas que sólo pueden ser ejecutados con esas versiones antiguas. La protección de estos sistemas inseguros no puede realizarse en la mayoría de casos con cortafuegos personales, y tiene que ser realizada más allá del perímetro del propio sistema.

Ante esta situación, surge el concepto de cortafuegos de red, definido como un equipo que se ubica en un punto de interconexión de subredes de una organización y que aplica criterios de filtrado al tráfico que lo atraviesa. Estos criterios pueden ser:

- Parámetros del flujo de tráfico implícitos en el tráfico.

- Usuario origen o destino del tráfico.

- Condiciones de entorno (hora, fecha, carga, etc.).

Las acciones de filtrado que se pueden ejecutar cuando se satisfacen los requisitos incluyen:

- Autorización de tráfico entrante o saliente.

- Bloqueo de tráfico entrante o saliente.

- Rechazo de tráfico entrante o saliente.

- Desvío de tráfico.

- Solicitud de autorización y/o autenticación.

De esta forma, en un único punto se puede configurar la protección de todo un conjunto de sistemas y subredes, independientemente de su tamaño y heterogeneidad, lo cual solventa en gran medida los inconvenientes de una protección individual de cada sistema, ya que la administración de la seguridad de una red se simplifica drásticamente, al tener un solo punto de configuración de la política de seguridad, siendo mucho más fácil su administración y evolución. Además, se mejora la capacidad de monitorización de la seguridad de la red, ya que sólo hay un punto expuesto a ataques y todos los ataques deben atravesar primero el cortafuegos, por lo que la vigilancia y monitorización es más sencilla que en el caso de la defensa perimetral de sistema. El objetivo de la defensa perimetral de red es aplicar una política de seguridad a un conjunto de sistemas en un único punto.

El primer paso que hay que llevar a cabo en la tarea de aplicación de la política de seguridad conjunta consiste en definir las zonas de seguridad.

5.2.1 Zonas de seguridad

Como se ha especificado anteriormente, el cortafuegos de red debe ubicarse en algún punto de la red de la organización que interconecte distintas zonas. Las zonas diferenciadas son las denominadas zonas de seguridad de la organización, y el cortafuegos impone la protección del perímetro de cada una de estas zonas. Lo primero que se debe realizar para configurar una arquitectura de red protegida por cortafuegos de red es la identificación de estas zonas, de forma que el cortafuegos se ubique en la frontera entre distintas zonas y pueda imponer la configuración de protección adecuada para cada una de las zonas. Es decir, dentro de cada una de las zonas definidas se aplica una política de seguridad común a todos los sistemas incluidos dentro de ella, impuesta por el cortafuegos correspondiente.

Para identificar las zonas de seguridad que existen en una organización, es necesario identificar conjuntos de sistemas y subredes a los que se les puede aplicar una configuración de seguridad uniforme a todos ellos. Aunque una configuración puede incluir un determinado número de excepciones, es recomendable que el número de excepciones sea lo más pequeño posible, por lo que es necesario que las zonas de seguridad estén compuestas por sistemas y subredes con los mismos o similares requisitos de protección [21].

El caso más simple es aquel en el que sólo se define una zona de seguridad interna, en el que todas las redes de una organización constituyen una zona de seguridad, y el resto de Internet es externo (Figura 31). En este caso, el cortafuegos se ubicaría en la conexión externa de las redes de la organización y se configuraría de una forma uniforme para todos los sistemas pertenecientes a la misma. Este tipo de zonificación tiene la ventaja de su simplicidad de administración, pero puede resultar demasiado rígido, así como necesitar la configuración de diversas excepciones.

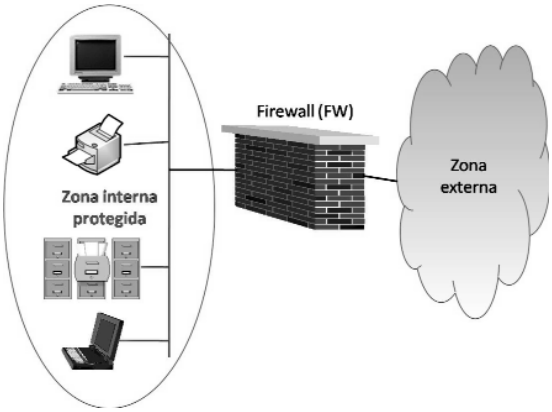

Figura 31: Cortafuegos de red con dos zonas de seguridad

Otro ejemplo es la configuración de dos zonas de seguridad dentro de la organización (Figura 32), una zona con una configuración de seguridad más estricta, y otra zona con una configuración más permisiva, de forma que el cortafuegos se ubica como interfaz entre estas dos zonas y también con la conexión externa (zona externa). De esta forma, la zona más segura tendrá una configuración de seguridad sin excepciones, y los equipos que necesiten una protección menos estricta se ubicarían en la segunda zona de seguridad.

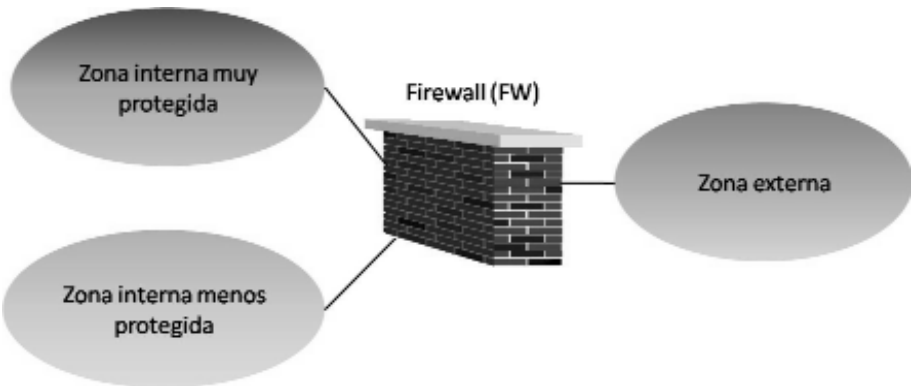

Figura 32: Cortafuegos de red con tres zonas de seguridad

Dependiendo de las necesidades de cada organización pueden identificarse otro tipo de zonas de seguridad, como por ejemplo, una zona de invitados, zona de investigación, etc. en las que el nivel de protección es distinto. En estos casos, será necesario ubicar uno o varios cortafuegos en las fronteras entre zonas.

5.2.2 Tipos de cortafuegos

El cortafuegos es un equipo que se ubica interconectando dos enlaces de red (por lo que debe tener al menos dos interfaces de red), que se encarga de aplicar la configuración de seguridad al tráfico que pretende atravesarlo en ambos sentidos. Al tener al menos dos conexiones de red, debe incluir una torre de protocolos que permita ejecutar los protocolos de Internet, en sus cuatro niveles: nivel de enlace, nivel de red, nivel de transporte y nivel de aplicación.

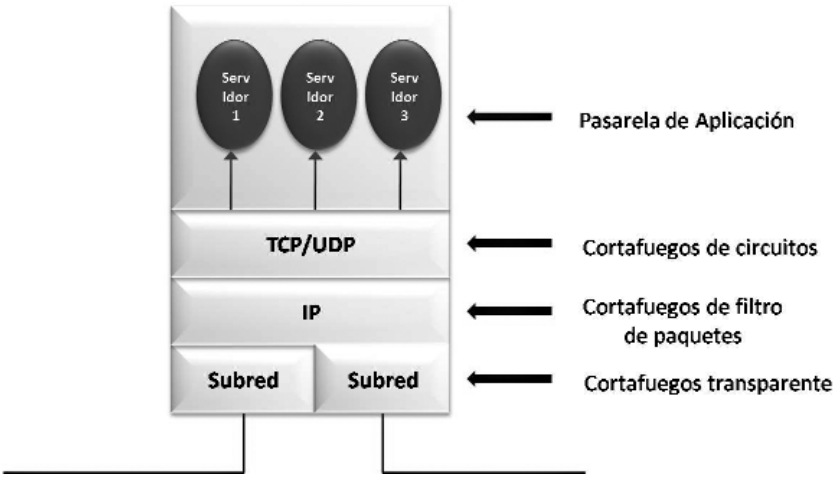

Figura 33: Tipos de cortafuegos de red

En función del nivel de la torre de protocolos del cortafuegos en el que se produzca el filtrado de tráfico, se pueden distinguir cuatro tipos de cortafuegos, tal como se ilustra en la Figura 33:

- Cortafuegos transparente: las funcionalidades de cortafuegos se incluyen en el nivel de enlace, actuando como un equipo puente (*bridge*) entre distintos segmentos pertenecientes a una misma subred.

- Cortafuegos de filtro de paquetes: las funcionalidades de cortafuegos se incluyen en el nivel de red, actuando como un encaminador de datagramas IP entre distintas subredes.

- Cortafuegos de circuitos: las funcionalidades de cortafuegos se incluyen en el nivel de transporte, conectando o desconectando distintas conexiones TCP o UDP entre sí.

- Pasarela de aplicación: las funcionalidades de cortafuegos se incluyen dentro de la capa de aplicación como un conjunto de servicios de aplicación que imponen la configuración de seguridad del cortafuegos.

Aunque se enuncian cuatro tipos de cortafuegos, en realidad sólo son dos tecnologías principales: filtro de paquetes, con su variación de cortafuegos transparentes, y pasarela de aplicación, con su variación de cortafuegos de circuitos. En las secciones siguientes se describen en detalle cada una de estas dos tecnologías [22].

5.2.2.1 Cortafuegos de filtro de paquetes

Este tipo de cortafuegos es el más simple y más utilizado, debido principalmente a la transparencia y nulo impacto que supone en el resto de infraestructura de red, ya que no es necesario modificarla por el hecho de implantar el cortafuegos.

Este tipo de cortafuegos, también denominado "*screening router*", actúa igual que un encaminador tradicional, aceptando datagramas IP que le llegan por sus enlaces y reencaminándolos por otros enlaces hacia otros destinos de acuerdo con una tabla de encaminamiento. La principal diferencia con un encaminador tradicional es que antes de consultar la tabla de encaminamiento, se consulta la configuración de seguridad y en base a parámetros del propio datagrama IP o parámetros de entorno, el datagrama es aceptado y encaminado hacia su destino, o bloqueado según especifique la configuración de seguridad [23].

Por ello, el cortafuegos de filtro de paquetes debe examinar los datagramas que llegan a él por cualquiera de sus interfaces y contrastarlos con la configuración de seguridad para determinar si el datagrama debe seguir su camino hasta su destino, según la tabla de encaminamiento, o debe ser bloqueado o tratado de alguna otra manera.

Parámetros de la configuración de seguridad

La configuración de seguridad se basa en contrastar parámetros de los datagramas IP, ya que el cortafuegos de filtro de paquetes actúa a nivel de red, donde se manejan los datagramas del protocolo IP y se tiene acceso a los campos presentes en la cabecera de estos datagramas. Estos campos incluyen la dirección IP origen y dirección IP destino del datagrama, que sin lugar a dudas resultan de gran utilidad para poder definir una configuración de seguridad en base al origen y el destino de los paquetes.

No obstante, excepto las direcciones IP origen y destino, la cabecera de los datagramas IP no incluye ninguna otra información que pueda ser de utilidad para incluir en una configuración de seguridad de un cortafuegos, ya que, por ejemplo, no aporta información acerca del tipo de aplicación que transporta dicho datagrama, lo cual resultaría de gran utilidad para definir configuraciones de seguridad, permitiendo controlar la utilización de servicios, a la vez que el origen y el destino de los mismos. Otro de los campos presentes en la cabecera de los datagramas IP contiene información relacionada con el tipo de protocolo de transporte que viaja en el contenido del datagrama IP (TCP, UDP, etc.), información que permite definir configuraciones de seguridad con las que se puede controlar el protocolo de transporte utilizado, pudiendo permitir o restringir el uso de TCP o UDP según desee el administrador, pero no resulta de utilidad en la práctica. El administrador de seguridad quiere controlar el tráfico no por el tipo de protocolo de transporte, que en pocos casos le resulta de utilidad, sino por el protocolo de aplicación que equivale al servicio final que transporta el datagrama IP, pero esta información no reside en la cabecera del datagrama IP sino en la cabecera de los paquetes de los protocolos de transporte (TCP y UDP). En concreto, en las cabeceras de los protocolos TCP y UDP se encuentra el campo "Destination Port", que contiene el tipo de aplicación que se transporta dentro de dichos protocolos, con valores como 80 para el protocolo de aplicación HTTP (servicio Web), 25 para el protocolo de aplicación SMTP (servicio de correo electrónico), etc. En base a estos valores sería posible definir una configuración de seguridad que filtrara por tipo de servicio.

Por ello, a pesar de que la funcionalidad del cortafuegos del filtro de paquetes reside en el nivel IP, es necesario que este cortafuegos se exceda en sus funciones y sea capaz de inspeccionar las cabeceras de los protocolos de transporte. De esta manera, el cortafuegos de filtro de paquetes debe ser capaz de procesar las cabeceras del protocolo IP, y acceder al contenido del datagrama IP para extraer el paquete del protocolo de transporte y ser capaz de procesar las cabeceras de dicho protocolo, bien sea TCP o UDP, para tener acceso al contenido del campo "*Destination Port*". Con la información contenida en este campo ya se puede implantar una configuración de seguridad basada en los servicios requeridos.

Tras lo enunciado en los párrafos anteriores, se concluye que los parámetros del datagrama IP accesibles, útiles para controlar el tráfico son los siguientes:

- Dirección IP origen (Campo IP *Source* de la cabecera del datagrama IP).

- Dirección IP destino (Campo IP *Destinatio*n de la cabecera del datagrama IP).

- Servicio (Campo "*Destination Port*" de la cabecera de los protocolos TCP y UDP).

Estos tres parámetros son los más importantes a la hora de definir configuraciones de seguridad, aunque es posible añadir alguno más incluido en la cabecera del datagrama IP, como los campos TOS (Type of Service) o el TTL (Time To Live), pero su uso es mucho más inusual en las configuraciones de seguridad. Algunos cortafuegos también tienen en cuenta parámetros de entorno, como la hora del día, o la carga de algún equipo.

Otro tipo de parámetro que se puede utilizar para la definición de reglas es el interfaz por el que llegan o salen los datagramas. De esta manera, es posible definir configuraciones de seguridad aplicables sólo a los datagramas que llegan al equipo, a los que llegan por un determinado interfaz, a los de salida, o a los que salen por un determinado interfaz. Sin embargo, la definición de seguridad utilizando este parámetro puede llegar a ser compleja y difícil de administrar, siendo mucho más recomendable la especificación de origen y destino en los campos correspondientes. No obstante, este parámetro es útil para las configuraciones de seguridad denominadas "*anti-spoofing*", en las que se trata de controlar los datagramas con direcciones fuente o destino falsificadas. En este caso, una configuración de seguridad recomendable debe incluir una regla que indique que por un interfaz externo a la organización no puede llegar un datagrama que tenga como dirección origen una dirección interna de la organización. Sin embargo, para simplificar la administración de la configuración de seguridad es recomendable que el resto de definiciones se basen en las direcciones origen y destino, en vez de en el interfaz de llegada/salida.

Un parámetro que podría resultar muy útil para la configuración de seguridad pero que no es posible utilizar en la práctica, es la identidad del usuario emisor o receptor del datagrama. En realidad, la utilización de direcciones IP origen o destino como parámetros de una configuración de seguridad es una simplificación que permite especificar a un usuario. La configuración de seguridad sería más completa si se dice que un usuario concreto puede usar el servicio X, en vez de indicar que una dirección IP puede conectarse al servicio X. Pero como no es posible extraer la identidad del usuario de un datagrama IP, se utilizan las direcciones IP como sucedáneo de dicho parámetro, con las limitaciones de seguridad que ello implica, como por ejemplo, el hecho de que la máquina puede estar siendo usada por otro usuario que no tiene permiso para conectarse al servicio X. La no utilización del filtrado basado en la identidad de los usuarios es la principal limitación de los cortafuegos de filtro de paquetes.

Acciones de la configuración de seguridad

La configuración de seguridad, tal y como se describió anteriormente, se basa en un conjunto de reglas. Cada regla contiene un conjunto de parámetros y una acción asociada. Cuando un datagrama llega al cortafuegos, se contrastan los parámetros de dicho datagrama con los parámetros de las reglas secuencialmente, hasta encontrar una regla cuyo conjunto de parámetros coincida con los del datagrama. En ese instante, se ejecuta la acción asociada a la regla, se pasa al siguiente datagrama y se realiza el mismo proceso.

Las acciones básicas asociadas a las reglas que se pueden ejecutar pueden ser:

- Aceptar. El datagrama es aceptado y se procesa encaminándolo hacia su destino.

- Rechazar. El datagrama no se procesa y se envía una notificación de rechazo al remitente usando el protocolo ICMP (ICMP Reject) normalmente.

- Tirar. El datagrama no se procesa y simplemente se descarta, sin notificar al originador.

La diferencia fundamental entre rechazar y tirar es que un rechazo es más "amable", ya que se informa al originador de que su datagrama ha sido rechazado, pudiendo éste tomar acciones inmediatas al respecto. Sin embargo, esto implica, de alguna forma, que se pueda desvelar la existencia del cortafuegos, ya que un encaminador tradicional no envía en situaciones normales este tipo de rechazos. Por otra parte, si el paquete se tira, no se infiere conocimiento de que existe un cortafuegos, pero implica que el originador se quede esperando respuesta a su petición hasta que salta el temporizador, lo cual ocasiona retardos considerables en el originador.

Además de las tres acciones definidas, los cortafuegos pueden llevar a cabo otro tipo de acciones, como la reescritura de los parámetros del datagrama (cambio de dirección IP fuente, destino, servicio, etc.) o el procesamiento por un servicio local del cortafuegos. Este tipo de funcionalidades se describirán con detalle más adelante en la sección de características avanzadas del cortafuegos.

Cortafuegos de inspección con estado

Como se ha mencionado anteriormente, el cortafuegos de tipo filtro de paquetes se basa en inspeccionar cada datagrama que llega al cortafuegos por sus interfaces y contrastarlo con los parámetros definidos en la configuración de seguridad para saber si es o no aplicable la acción correspondiente. Sin embargo, tener que inspeccionar todos los datagramas cuando se transmite a grandes velocidades puede ser una labor muy compleja y podría limitar las prestaciones de las redes. Por ello, la opción más adecuada es seguir la denominada inspección con estado (*stateful packet inspection*), por la cual sólo se comparan con la configuración de seguridad aquellos datagramas que suponen una petición de conexión. Si el datagrama es aceptado, el cortafuegos registra la conexión y acepta también el resto de datagramas posteriores que pertenecen a dicha conexión. Si el datagrama es rechazado, la conexión no puede ser establecida, por lo que no se aceptan datagramas posteriores de dicha conexión, sólo nuevos intentos de la misma que se volverán a contrastar con la reglas.

Esta tecnología permite que la configuración de seguridad se defina teniendo en cuenta sólo las peticiones de conexión, sin tener que definir una configuración de seguridad adicional para las respuestas. Es decir, si el cortafuegos acepta una conexión de A (equipo externo) a B (equipo interno), ya que la configuración de seguridad así lo especifica, todos los paquetes posteriores que pertenecen a la misma conexión, bien sean desde A hacia B o desde B hacia A son aceptados sin ser contrastados con la configuración de seguridad, lo cual permite aumentar drásticamente las prestaciones y la velocidad del cortafuegos.

Los cortafuegos de inspección de estado funcionan a partir de la base de que son capaces de registrar una petición de conexión aceptada, y de identificar paquetes posteriores como pertenecientes a dicha conexión. Sin embargo, esto no siempre es una tarea sencilla. Servicios que se basan en el protocolo de transporte TCP, como la web o el correo electrónico (HTTP y SMTP) son conexiones sencillas de identificar, ya que el protocolo TCP es un protocolo orientado a conexión y tiene implícito el concepto de sesión. Sin embargo, servicios basados en el protocolo de transporte UDP, como por ejemplo el servicio de nombre de internet (DNS), resultan más complejos de identificar, ya que UDP no es un protocolo orientado a conexión, y solicitudes consecutivas o incluso peticiones y respuestas asociadas, no están ligadas bajo ningún concepto de sesión o conexión, por lo que el cortafuegos debe incluir métodos que permitan emular el concepto de sesión para este tipo de servicios, como por ejemplo apuntar las direcciones origen y destino y el servicio, y establecer un temporizador para aceptar paquetes en sentido inverso como respuestas

a peticiones previas. Otros servicios ofrecen también dificultades debido a su diseño, como el servicio de transferencia de ficheros (FTP), que se conecta a puertos arbitrarios como parte de una misma conexión. Los cortafuegos deben ser capaces de tratar la problemática asociada a la identificación de conexiones en estos servicios "especiales" de una forma particular para cada servicio.

Configuración de seguridad

El cortafuegos de tipo filtro de paquete se basa en contrastar los parámetros de los datagramas de solicitud de conexión con una lista de configuraciones de seguridad. Cada configuración de seguridad está compuesta por un conjunto de parámetros que deben cumplir los datagramas y una acción asociada en caso de que el datagrama cumpla dichos parámetros. Esta configuración constituye las denominadas reglas de un cortafuegos.

Las reglas de un cortafuegos expresan la política de seguridad que va a imponer dicho cortafuegos a las solicitudes de conexión que lo atraviesan. Como se indicó anteriormente, cada solicitud de conexión es contrastada con las reglas del cortafuegos secuencialmente, hasta encontrar una regla cuyos parámetros coinciden con los del datagrama analizado. En ese caso, se ejecuta la acción asociada a dicha regla y se continúa con el siguiente paquete realizando el mismo proceso.

Por ello, la definición de las reglas de un cortafuegos es una de las tareas más críticas en la implantación de una política de seguridad de red. Una incorrecta definición de reglas puede abrir agujeros de seguridad explotables remotamente. Asimismo, una definición de reglas muy extensa puede llevar a dificultades de administración de dicha política de seguridad y disminución de las prestaciones del cortafuegos. Por lo tanto, la definición de las reglas debe ser lo más concisa y precisa posible por una parte, y, por otra, no debe dejar ningún hueco sin cubrir por la política de seguridad.

Existen muchas formas de definir reglas de cortafuegos, y cada administrador de seguridad suele aplicar su propio método para definirlas. Sin embargo, es necesario ser muy cuidadoso con la definición de reglas, ya que una regla mal definida o mal situada puede afectar a la seguridad global del sistema.

Para definir una política de seguridad basada en reglas de un cortafuegos es necesario, en primer lugar, conocer cuáles son las zonas de seguridad que separa dicho cortafuegos, y cuáles son los flujos de tráfico permitidos y restringidos entre dichas zonas. Por ejemplo, supongamos que se quiere expresar la siguiente política de seguridad:

1. No se permiten conexiones de la zona A (externa) a la zona B (interna).

2. Sólo se permiten conexiones de Web y de correo de la zona B (interna) a la zona A (externa).

Dicha política de seguridad puede ser expresada mediante un conjunto formado por tres reglas de seguridad (el segundo punto de la política será definido mediante dos reglas):

1. No se permiten conexiones de la zona A (externa) a la zona B (interna).

2. Se permiten conexiones de Web y de correo de la zona B (interna) a la zona A (externa).

3. No se permiten conexiones de la zona B (interna) a la zona A (externa).

Debe notarse que la tercera regla contradice a la anterior. Sin embargo, como las reglas son comprobadas secuencialmente, una conexión Web saliente satisfará la segunda regla, cuya acción (aceptar) será ejecutada sin llegar a comprobar la siguiente regla.

Por otra parte, es necesario comprobar que las reglas cubren todos los flujos de tráfico en el cortafuegos. Por ejemplo, si se define una política de seguridad con las siguientes reglas:

1. Se permiten conexiones de Web de la zona A (externa) al servidor X de la zona B (interna).

2. Se permiten conexiones de correo de la zona A (externa) al servidor Y de la zona B (interna).

3. No se permiten conexiones de la zona A (externa) a la zona B (interna).

Esta política de seguridad restringirá el tráfico entrante para sólo permitir el servicio Web y el correo electrónico a los servidores correspondientes, pero no cubre todos los flujos de tráfico, ya que no se contempla ninguna regla para el tráfico de salida de la organización. Por ello, una conexión de salida que vaya de la zona B (interna) a la zona A (externa) no será identificada por ninguna regla, por lo que el cortafuegos comprobará hasta la última regla sin poder aplicar ninguna a dicha conexión. En ese caso, el cortafuegos normalmente descarta la conexión. Esta acción por defecto de

los cortafuegos se incluye precisamente para combatir las políticas de seguridad mal expresadas. Si no hay ninguna regla que afecte a una solicitud de conexión, ésta se descarta. Por lo tanto, la configuración de seguridad anterior debe ser expresada correctamente de la siguiente manera:

1. Se permiten conexiones de la zona B (interna) a la zona A (externa).

2. Se permiten conexiones de Web de la zona A (externa) al servidor X de la zona B (interna).

3. Se permiten conexiones de correo de la zona A (externa) al servidor Y de la zona B (interna).

4. No se permiten conexiones de la zona A (externa) a la zona B (interna).

Como se deduce del análisis de los ejemplos anteriores, es muy aconsejable seguir alguna metodología en la definición de las reglas de seguridad de un cortafuegos. De esta forma su mantenimiento y evolución podrán realizarse con mayores garantías de no incurrir en algún error que abra un agujero de seguridad. Por otra parte, los cortafuegos más modernos incluyen un verificador de reglas que evalúa la incompatibilidad de reglas, pero no pueden detectar muchos fallos en las configuraciones que pueden darse por una incorrecta definición de las reglas de seguridad. Una de las metodologías más utilizadas para la definición de las reglas es dividir el conjunto de reglas en tres categorías que deben ser definidas en el orden en que se presentan:

1. Reglas de autoprotección del cortafuegos, diseñadas para controlar el acceso al propio cortafuegos.

2. Reglas de salida, que regulan el tráfico desde la zona interna hacia el exterior.

3. Reglas de entrada, que regulan el tráfico desde la zona externa hacia el interior.

En las secciones posteriores se exponen las principales características de cada uno de los conjuntos de reglas anteriores.

Reglas de autoprotección

El primer conjunto de reglas son aquellas cuyo objetivo es controlar el tráfico dirigido al propio cortafuegos, es decir, tráfico que no está destinado a atravesar el cortafuegos, sino que tiene como destino final el propio cortafuegos, en alguno de sus servicios. Este tráfico es en sí anormal, ya que a excepción de un administrador nadie debería conectarse a un cortafuegos como destino final, puesto que el cortafuegos de filtro de paquetes no debe ofrecer servicios a usuarios finales. Por lo tanto, es muy recomendable que las reglas de autoprotección se reduzcan a una:

- Se prohíbe el tráfico desde cualquier origen y para cualquier servicio que tenga como destino el cortafuegos.

De esta forma, se asegura la autoprotección del propio cortafuegos, ya que éste va a descartar cualquier intento de conexión a los servicios de administración que pueda tener. Sin embargo, la regla anterior tiene el efecto lateral de que se restringen también las conexiones de administración remota del cortafuegos. Por ello, en teoría, el cortafuegos debe ser administrado por consola local, no permitiendo conexiones al mismo ni para su administración remota. No obstante, esta teoría puede resultar demasiado incómoda en ciertos entornos, en los que se pueden habilitar excepciones muy controladas para su administración remota.

Reglas de salida

El segundo conjunto de reglas controla el tráfico de salida, es decir, tráfico generado en la zona interna protegida y dirigido hacia la zona externa. Las reglas de salida se encargan de controlar el tráfico generado por los usuarios de la organización que va dirigido al exterior. Para la definición de las reglas de salida, existen dos opciones:

- Opción permisiva. No se restringen las conexiones hacia el exterior de los usuarios de la organización, excepto las expresamente prohibidas. Sigue la filosofía de "Excepciones prohibidas, resto de conexiones de salida permitidas".

- Opción restrictiva. Se prohíbe, por norma general, toda conexión hacia el exterior, excepto las expresamente permitidas. Sigue la filosofía de "Excepciones permitidas, resto de conexiones de salida prohibidas".

Cualquiera de las dos opciones consta de dos partes: un conjunto de excepciones y una regla general (permitida o prohibida por defecto). Es muy importante incluir la regla general aunque sea duplicada posteriormente para evitar cualquier tipo de desajuste en la definición de reglas.

Las opciones anteriores se expresarían en forma de reglas de la siguiente forma:

- Opción permisiva:
  - Se prohíben determinadas conexiones desde la zona interna a la zona externa (ciertos servicios, ciertas direcciones origen o destino, etc.).
  - Se permiten todas las conexiones desde la zona interna a la zona externa (Regla general).
- Opción restrictiva:
  - Se permiten determinadas conexiones desde la zona interna a la zona externa (ciertos servicios, ciertas direcciones origen o destino, etc.).
  - Se prohíben todas las conexiones desde la zona interna a la zona externa (Regla general).

El control del tráfico de salida no se realiza para evitar ataques desde el exterior, sino para el control de las conexiones de los usuarios, para evitar la utilización indebida de la conexión a Internet por parte de los usuarios de la organización. Aunque de forma colateral, este control puede bloquear intentos de acceso al exterior por parte de equipos infectados con programas maliciosos, como caballos de Troya, *spyware*, etc.

Reglas de entrada

El tercer conjunto de reglas controla el tráfico de entrada, es decir, tráfico generado en la zona externa y dirigido hacia la zona interna. Las reglas de entrada se encargan de controlar el tráfico que llega a la organización desde el exterior, supuesto una división básica en zonas de seguridad en la que el cortafuegos separa la zona interna (organización) de la conexión al exterior. Teóricamente, para la definición de las reglas de entrada existen también las dos opciones permisiva y restrictiva especificadas en las reglas de salida. Pero en la práctica, la opción permisiva no debe aplicarse

nunca para el tráfico de entrada, ya que es mucho más peligroso que el tráfico de salida, y la aplicación de una regla general mediante la que se permita todo el tráfico que no esté expresamente prohibido, abriría muchas vías de acceso a nuestro sistema que podrían comprometer la seguridad de la organización.

Por ello, la definición de las reglas de entrada podría ser la siguiente:

- Se permiten determinadas conexiones desde la zona externa a la zona interna (ciertos servicios, ciertas direcciones origen o destino, etc.).

- Se prohíben todas las conexiones desde la zona externas a la zona interna (Regla general).

En general, las excepciones de entrada son potenciales agujeros de seguridad, por lo que es necesario evitarlas siempre que sea posible. Sin embargo, muchas veces es necesaria su inclusión (acceso desde el exterior a un servidor Web o de correo electrónico, por ejemplo), por lo que en estos casos la excepción debe limitarse a especificar exactamente las direcciones destino permitidas, y los únicos servicios accesibles en dichos destinos.

La última regla general de una política de seguridad (la regla general para el tráfico de entrada) puede ser expresada también como una regla de prohibición total, es decir, se podría expresar diciendo que todo el tráfico que alcance dicha regla es rechazado, para cualquier origen, destino o servicio. De esa forma, se asegura que no hay ningún tráfico que no se vea afectado por la definición de reglas del cortafuegos y se evita la entrada de tráfico no permitido. De hecho, en muchos cortafuegos esta regla la pone por defecto el propio cortafuegos. El hecho de incluirla explícitamente en el cortafuegos puede permitir la generación adicional de registros y *logs*, que pueden ser de utilidad para analizar el tráfico rechazado por el cortafuegos.

Un ejemplo de la definición de los tres conjuntos de reglas especificados puede verse en la Figura 34, en la que se muestra la captura de un interfaz de definición de reglas de un cortafuegos comercial.

Figura 34: Interfaz de definición de reglas de un cortafuegos comercial

5.2.2.2 Cortafuegos transparentes

Los cortafuegos transparentes, también denominados cortafuegos de nivel de enlace, constituyen una variación del cortafuegos de filtro de paquetes visto anteriormente. Si los cortafuegos de filtro de paquetes actúan como un encaminador, aceptando datagramas IP y encaminándolos por el enlace correspondiente según la tabla de encaminamiento hacia otra subred IP, el cortafuegos transparente actúa como una pasarela de nivel de enlace, lo que se conoce tradicionalmente como un "*bridge*". Los *bridges* son equipos que interconectan dos o más enlaces y encaminan tramas de nivel de enlace entre ellos. Estos equipos han sido sustituidos actualmente por otro tipo de equipos, como los conmutadores (*switches*).

El hecho de recuperar este tipo de tecnología para su utilización como cortafuegos radica en que este equipo funciona a nivel de enlace, encaminando tramas de nivel de enlace según las direcciones físicas, por lo que no necesita tener nivel de red, transporte o aplicación. Por ello, si el equipo no tiene nivel de red, no soporta el protocolo IP y consecuentemente, no tiene dirección IP asociada. Esta es la principal ventaja de este tipo de cortafuegos (y de ahí su nombre, cortafuegos transparente), ya que al no tener una dirección IP, este cortafuegos es "indetectable" para un atacante

remoto que esté en otra subred distinta a la del cortafuegos. Un cortafuegos de filtro de paquetes tiene una dirección IP que un atacante puede averiguar y, como consecuencia, intentar una serie de ataques dirigidos contra el propio cortafuegos (motivo por el cual en las definiciones de reglas las primeras reglas son las de autoprotección del cortafuegos).

Por lo tanto, el cortafuegos transparente actúa como un bridge que interconecta normalmente dos enlaces Ethernet (pertenecientes a una misma subred IP), pero que, a diferencia de éste, inspecciona las tramas de nivel de enlace antes de encaminarlas por el enlace correspondiente, como se ilustra en la Figura 35. Por ello, este tipo de cortafuegos no puede comparar solamente los parámetros que se encuentran en la cabecera de los protocolos de enlace, como hacen los bridges tradicionales, sino que deben ser más inteligentes y ser capaces de procesar el contenido de las tramas de enlace en busca de los paquetes IP y los parámetros de su cabecera, y de los paquetes TCP o UDP que se transportan en busca de los campos útiles como parámetros de filtrado, de la misma forma que se vio en los cortafuegos de filtro de paquetes.

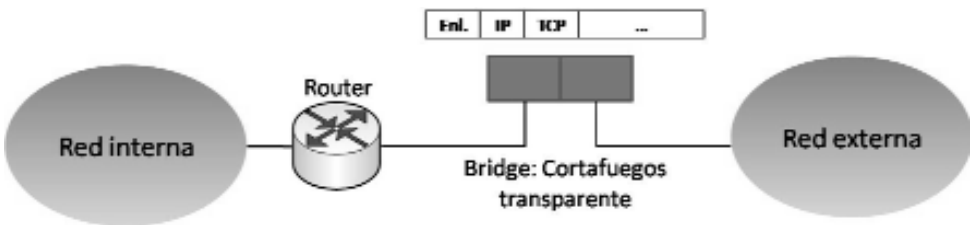

Figura 35: Cortafuegos transparente

Además de la ventaja que implica el ser transparente a nivel IP, este cortafuegos tiene las mismas características, ventajas y limitaciones que los cortafuegos de filtro de paquetes vistos anteriormente.

5.2.2.3 Pasarelas de aplicación

Estos cortafuegos constituyen la otra gran tecnología de cortafuegos, junto a la de filtro de paquetes. En una pasarela de aplicación, la funcionalidad de cortafuegos se realiza a nivel de aplicación, en un conjunto de servidores (pasarelas de aplicación o proxy de aplicación) que aplican la configuración de seguridad a las conexiones que llegan a ellos.

Una pasarela de aplicación es un cortafuegos con dos o más enlaces conectados a distintas subredes, que recibe datagramas IP por uno de sus enlaces, pero NO hace encaminamiento a nivel IP en ningún momento, siendo ésta la característica principal de estos cortafuegos. Este hecho es una paradoja en la arquitectura de Internet, ya que supone en la práctica un corte en las comunicaciones IP ya que no existe conectividad entre las subredes interconectadas por el cortafuegos. Un datagrama enviado desde un equipo interno con destino un equipo externo, será encaminado hasta llegar al cortafuegos donde se tirará, ya que el cortafuegos no lo encaminará a nivel IP hacia su destino final. Por lo tanto, este tipo de cortafuegos corta las comunicaciones que intentan atravesarlo. La única forma de atravesar el cortafuegos pasa por establecer una comunicación desde el origen con el propio cortafuegos indicando el destino final de la conexión, que el cortafuegos establezca una conexión con el destino requerido, y que a nivel de aplicación el cortafuegos junte estas dos conexiones, tal y como se muestra en la Figura 36.

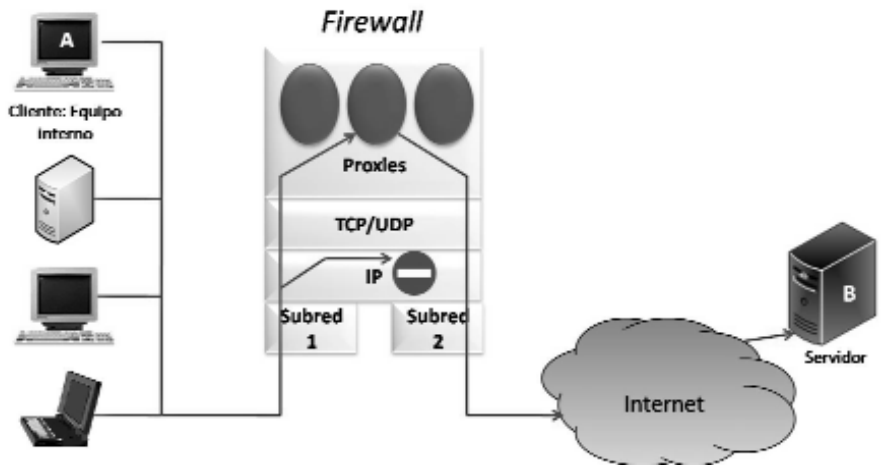

Figura 36: Pasarela de aplicación

No existe conectividad directa entre las redes interna y externa, por lo que un equipo interno que quiera establecer una conexión con un equipo externo, deberá primero establecer una conexión con el cortafuegos, negociar con un servicio del cortafuegos (la pasarela de aplicación), y si la pasarela permite la conexión, establecer una conexión desde la pasarela hasta el equipo remoto requerido. De esta manera, la pasarela conecta las dos conexiones a nivel de aplicación. Por tanto, la conexión se hace efectiva en dos pasos: cliente-pasarela y pasarela-servidor, siendo necesario una pasarela por servicio.

Esta tecnología presenta una serie de ventajas e inconvenientes, que a continuación se presentan.

La principal ventaja respecto a los cortafuegos de filtro de paquetes radica en la flexibilidad que tienen estos cortafuegos para establecer los parámetros de la configuración de seguridad, puesto que el equipo interno debe establecer una conexión con la pasarela de aplicación y negociar la conexión que requiere. En esta negociación la pasarela de aplicación puede imponer los criterios que desee, como por ejemplo, dirección fuente, dirección destino, hora, etc. (parámetros similares a los especificados en los cortafuegos de filtro de paquetes), y lo que es más importante, identidad del usuario. Las pasarelas, en respuesta a una petición de conexión remota, pueden solicitar el nombre del usuario y su clave, y aplicar este criterio como un parámetro más de filtrado, permitiendo establecer configuraciones de seguridad mucho más detalladas. Se puede realizar filtrado por identidad de usuario, a diferencia de los cortafuegos de filtro de paquetes en los que no era posible.

Además, las pasarelas de aplicación son específicos de cada servicio, es decir, existe una pasarela para conexiones Web, otra pasarela para conexiones FTP, etc., de forma que cada pasarela puede imponer unos parámetros y una negociación específica para cada tipo de servicio concreto, dotando de mayor expresividad a las configuraciones de seguridad.

Por otra parte, el hecho de que el cortafuegos aísle las redes que interconecta a nivel IP, permite que las redes internas no tengan conexión directa a Internet, por lo que se puede utilizar un plan de direccionamiento IP privado. En efecto, ninguna de las direcciones internas son visibles en Internet; la única dirección IP visible será la del interfaz externo del cortafuegos. Además, el hecho de no existir conexión directa a Internet desde el interior de la organización, dota de mayor seguridad al sistema.

Sin embargo, este tipo de cortafuegos tiene un gran inconveniente, y es que no respeta la arquitectura de Internet, por lo que es necesario aplicar

parches para su correcto funcionamiento. El principal parche que implican estos cortafuegos es la utilización de aplicaciones específicas, ya que el uso de aplicaciones normales no es válido. Una aplicación normal de Internet intentará establecer conexiones extremo a extremo, por lo que el cortafuegos bloqueará esa conexión. Es necesario que la conexión se realice en dos pasos:

- Conexión cliente-cortafuegos, en la que se establece la negociación de seguridad necesaria.

- Conexión cortafuegos-servidor, donde se puentean ambas conexiones a nivel de aplicación.

Por tanto, se pone de manifiesto la necesidad de clientes específicos, que tengan capacidad de soportar el acceso vía pasarela, ya que la mayoría de los clientes tradicionales no soportan este tipo de conexión. Este hecho hace que este tipo de cortafuegos se utilice sólo en entornos restrictivos con la conexión desde la organización hacia el exterior, ya que sólo aquellos servicios que tengan asociado una pasarela de aplicación pueden ser utilizados por los usuarios de la organización. El cortafuegos bloqueará todas las conexiones de entrada a la organización. Una conexión de entrada sólo podría ser realizada si el origen externo estableciera la conexión en dos pasos, lo cual es en la práctica imposible si la organización pretende proporcionar servicios anónimos y universales como un servidor Web, ya que no se puede imponer al resto de usuarios de Internet que para visitar un determinado servidor Web se deban modificar las configuraciones de conexión de su equipo. Por lo tanto, este tipo de cortafuegos se utiliza cuando no existe ningún requisito de conexiones entrantes que deban ser permitidas, es decir, es imposible utilizar este tipo de cortafuegos si se tienen servidores públicos dentro de la organización, puesto que no se puede acceder a ellos.

La utilización de clientes especiales restringe también la utilización de servicios, es decir, sólo se pueden utilizar aquellos servicios para los que existan pasarelas y clientes adaptados para la utilización de la pasarela de aplicación. Existen muchos servicios que pueden ser utilizados con clientes adaptados. Un claro ejemplo es el servicio de web y los navegadores, los cuales se pueden configurar para la utilización de pasarela de aplicación Web. Muchos otros servicios tienen clientes que pueden ser adaptados para su utilización con pasarela; es ya frecuente encontrar en las opciones de los clientes una sección dedicada a su uso con cortafuegos de nivel de aplicación, incluidos servicios P2P, TELNET, SSH, etc.

5.2.2.4 Cortafuegos de circuitos

El cortafuegos de circuitos, o cortafuegos de nivel de transporte, es una variación del cortafuegos de pasarela de aplicación. A pesar de estar ubicado en el nivel de transporte, se trata de un cortafuegos de nivel de aplicación basado en el concepto de pasarela de aplicación visto en los cortafuegos anteriores. La principal diferencia con las pasarelas de aplicación es que en este caso, existe una única pasarela servidora que se encarga del filtrado de todos los servicios, por lo que la configuración de seguridad de cada servicio ya no puede ser específica, a diferencia del caso anterior en el que los parámetros de filtrado podían variar en función del servicio. En los cortafuegos de circuitos sólo existe una pasarela genérica que aplica la configuración de seguridad a todos los servicios de la misma forma, utilizando el mismo conjunto de parámetros (Figura 37). Estos parámetros incluyen, además de los parámetros usuales como las direcciones IP origen y destino, servicio, etc., la posibilidad de solicitar autenticación al originador de la conexión y aplicar la identidad del usuario como parámetro de configuración de seguridad.

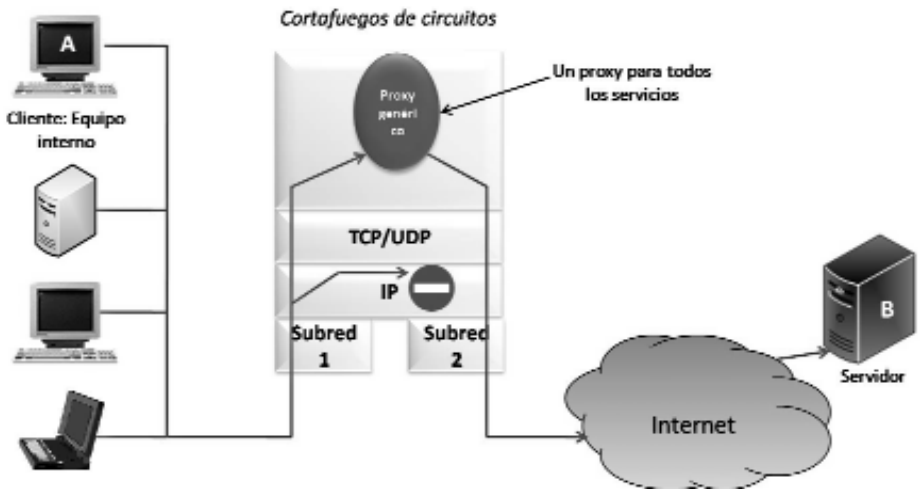

Figura 37: Cortafuegos de circuitos

Los cortafuegos de circuitos también se conocen como SOCKS (abreviatura de SOCKetS), nombre del popular producto gratuito que incluye el concepto de pasarela genérica.

5.2.3 Arquitecturas de red con cortafuegos

A la hora de diseñar la topología de una red que necesita protección con un cortafuegos, es necesario combinar tres elementos:

- El propio cortafuegos, que efectúa las labores de filtrado utilizando cualquiera de las cuatro tecnologías expuestas.

- El router de acceso al exterior de la organización.

- El conjunto de servicios que deben ser proporcionados al exterior y que, por lo tanto, deben estar accesibles desde el exterior. Los servidores que se encargan de proporcionar estos servicios no pueden ser protegidos en su totalidad, constituyen uno de los puntos más débiles de la red de la organización, y reciben el nombre de bastiones.

Las diferentes combinaciones de estos tres elementos dan lugar a distintas arquitecturas de red protegida con cortafuegos.

5.2.3.1 Arquitectura "Dual-homed host"

La arquitectura *Dual-homed host* es la arquitectura más simple y barata. Consiste en incluir los tres elementos mencionados en un solo equipo, tal y como puede verse en la Figura 38.

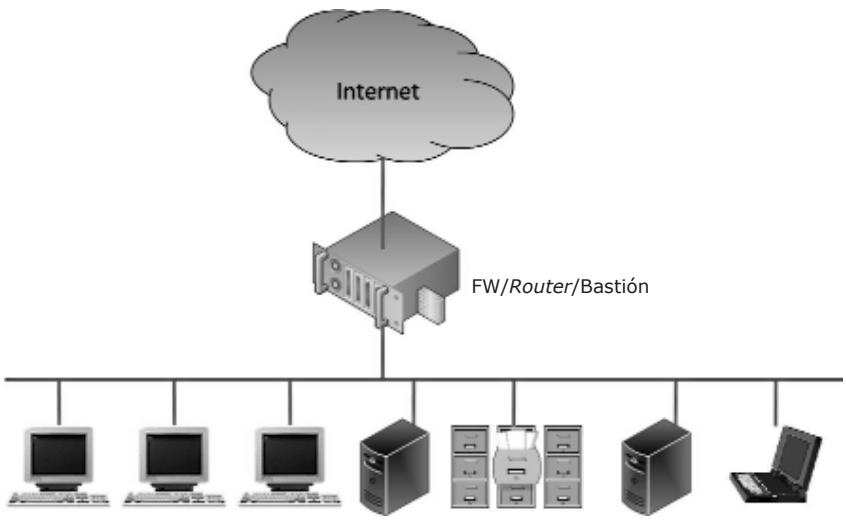

Figura 38: Arquitectura *Dual-homed host*

En esta arquitectura, no se tiene necesidad de interconexión desde el exterior hacia el interior, por lo que el cortafuegos puede ser de tecnología de circuitos o pasarela de aplicación, además de filtro de paquetes. El nivel de aplicación del propio cortafuegos albergará los servicios públicos que la organización ofrecerá al exterior (Web, mail, DNS, etc.). Si es de tipo pasarela de aplicación, su nivel de aplicación también albergará las pasarelas que se hayan configurado. Si es de tipo filtro de paquetes, deberá ser configurado con las excepciones necesarias para poder llegar a los servicios públicos albergados en el propio cortafuegos.

Esta arquitectura presenta graves problemas desde el punto de vista de la seguridad, debido a que las funciones de cortafuegos y de bastión residen en la misma máquina, es decir, se unen en la misma máquina cortafuegos y servidores públicos. Los servidores públicos son accesibles desde el exterior, y por lo tanto son vulnerables a ataques. Si un ataque a estos servidores se realiza con éxito, el atacante estará dentro del propio cortafuegos, lo que le permitirá acceder desde allí al interior de la organización y modificar la configuración del cortafuegos a su medida.

5.2.3.2 Arquitectura "Screened Host"

La arquitectura *Screened host*, expuesta en la Figura 39, combina las funcionalidades de cortafuegos y de *router* de acceso, separando los bastiones en máquinas independientes que deberán ser declaradas explícitamente en la configuración de seguridad. Es decir, se tienen por un lado en la misma máquina cortafuegos y *router* de acceso, y por otro, los bastiones.

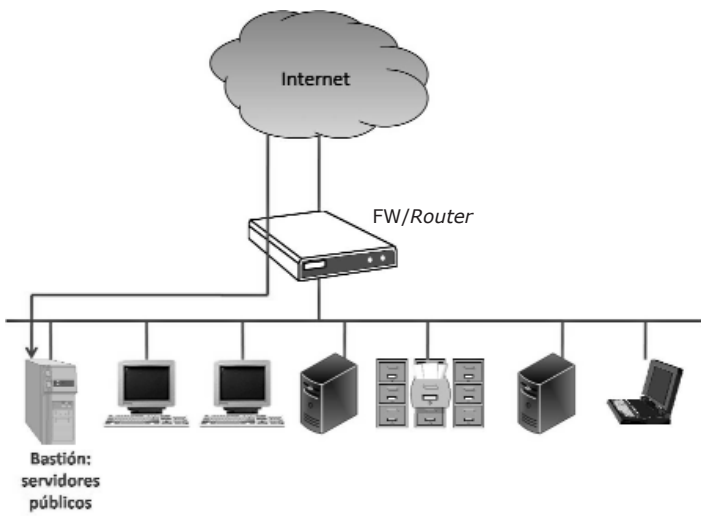

Figura 39: Arquitectura *Screened host*

El cortafuegos en este tipo de arquitectura debe ser de filtro de paquetes, no siendo aplicable el cortafuegos de pasarela de aplicación ya que, en este caso, sí es necesario efectuar conexiones desde el exterior hacia los bastiones que están ubicados en la zona protegida de la organización. La configuración de este cortafuegos debe incluir unas reglas de seguridad que permitan únicamente las conexiones hacia los servicios accesibles de los bastiones, restringiendo el resto de conexiones hacia el interior.

Esta arquitectura es más segura que la anterior, ya que permite la autoprotección del cortafuegos, impidiendo que un atacante acceda al cortafuegos y pueda modificar su configuración de seguridad. Sin embargo, sigue presentando problemas de seguridad en el caso de que un atacante sea capaz de atacar a algún servidor de los bastiones (ya que el cortafuegos debe permitir este tipo de conexiones). Desde allí, se tiene acceso al resto de la red interna sin que el cortafuegos lo impida. Es decir, si se ataca el bastión, es mucho más fácil acceder desde allí a los servidores internos de la organización, ya que el cortafuegos no actúa en este tipo de conexiones.

5.2.3.3 Arquitectura "Screened subnet"

En la arquitectura *Screened-subnet*, se separan las tres funcionalidades necesarias en tres máquinas distintas, una para el router, otra para el cortafuegos y otra para el bastión que alberga los servicios. Esta es la solución más costosa, ya que necesita más infraestructura en cuanto al número de máquinas, y más compleja desde el punto de vista de la topología de red, ya que es necesario añadir una nueva red entre el *router* de acceso a Internet y el cortafuegos. Esta red debe albergar los servicios accesibles desde el exterior, de forma que en la zona interna no debe residir ninguno de estos servicios, como se ilustra en la Figura 40. Por ello, el cortafuegos no tiene ninguna excepción de entrada configurada, y prohíbe toda conexión entrante procedente del exterior. En esta arquitectura el cortafuegos puede estar basado en cualquiera de las tecnologías ya expuestas, ya sea de filtro de paquetes o de pasarela de aplicación.

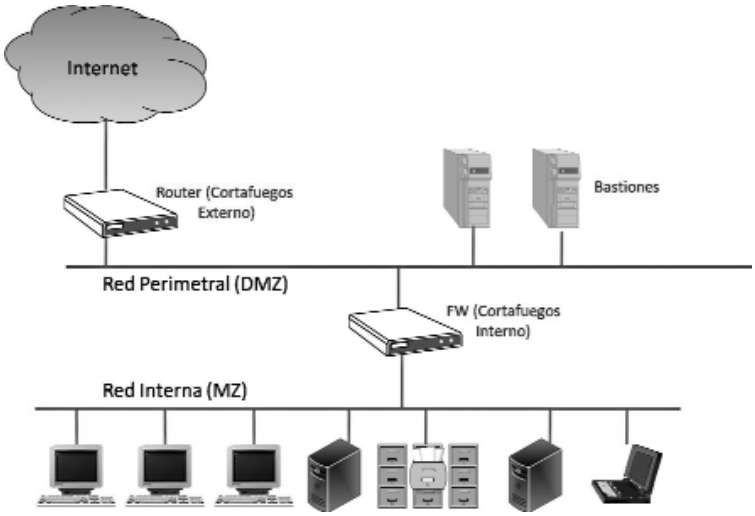

Figura 40: Arquitectura *Screened-subnet*

Esta arquitectura es la más recomendable desde el punto de vista de seguridad a cambio de una mayor inversión económica, ya que, a pesar de que los bastiones siguen siendo vulnerables a posibles ataques y no están protegidos, un ataque a los bastiones no implica ningún otro riesgo de seguridad adicional. Esto se debe a que desde los bastiones no se puede acceder a la red interna ya que el cortafuegos lo impide. La subred donde se ubican los bastiones entre el *router* externo y el cortafuegos se denomina Red Perimetral o Zona Desmilitarizada (DMZ según sus iniciales en inglés), en contraposición a la zona interna protegida que se denomina Zona Militarizada (MZ).

El *router* externo puede ser sustituido por un cortafuegos de filtro de paquetes que permita solamente las conexiones necesarias a los bastiones, incrementado el nivel de seguridad y ofreciendo una protección adicional a los bastiones.

Existe una variante de esta arquitectura que permite combinar las funcionalidades de cortafuegos y *router* externo. Consiste en un cortafuegos con tres enlaces, uno hacia el exterior, otro hacia el interior y un último interfaz hacia la red perimetral, tal y como se muestra en la Figura 41.

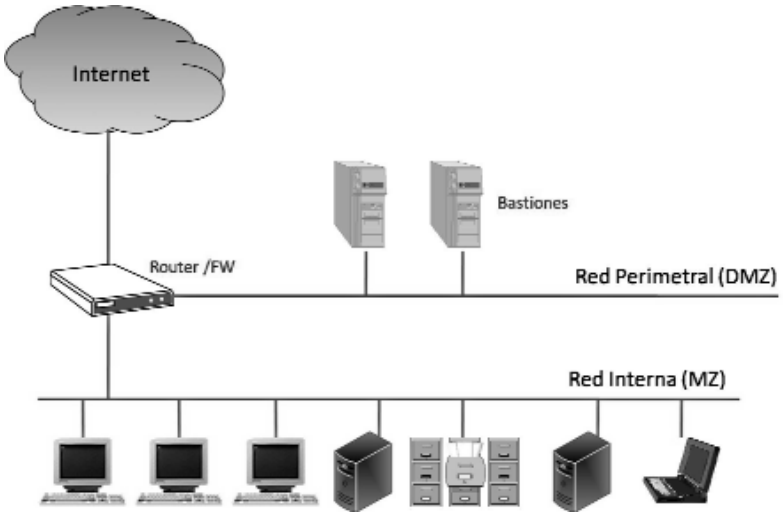

Figura 41: Variante de la arquitectura *Screened-subnet*

El principal inconveniente de esta variación es que es necesario ser muy cuidadoso con la configuración del cortafuegos para permitir y denegar los flujos de tráfico apropiados entre sus tres interfaces.

5.2.4 Características avanzadas de cortafuegos

Hasta ahora, se ha analizado el cortafuego desde el punto de vista de su funcionalidad básica, el filtrado de conexiones en base a una política de seguridad expresada en forma de reglas. Gracias a esta funcionalidad, el cortafuegos se ha convertido en un elemento esencial en la arquitectura de seguridad de red de las organizaciones, motivo por el que poco a poco se ha ido enriqueciendo en cuanto a funcionalidades y ha ido asumiendo otro tipo de funciones relacionadas con la seguridad. A continuación se presentan las funcionalidades más relevantes.

5.2.4.1 Cifrado de datos en tránsito

Las tecnologías de Redes Privadas Virtuales [24] han supuesto para muchas organizaciones un gran ahorro de costes, al poder interconectar distintas sedes remotas entre sí de una forma sencilla y barata, a la vez que se ofrecen capacidades de conexión remota a los teletrabajadores de una forma segura.

La Red Privada Virtual sustituye al concepto de Red Privada, en la que una organización utilizaba infraestructuras de comunicaciones en exclusividad para interconectar distintas sedes. Este alquiler de infraestructura suponía unos costes muy elevados para la organización, que en muchos casos no se veían compensados con los beneficios obtenidos por la interconexión. Este es el marco en el que surge el concepto de Red Privada Virtual, que se basa en utilizar redes compartidas, como Internet, para el intercambio de datos entre sedes remotas, en vez de utilizar infraestructuras de comunicaciones dedicadas para interconectar dichas sedes. Sólo es necesario que cada sede de la organización tenga una conexión a Internet para intercambiar datos entre ellas. Este escenario supone un gran ahorro de costes para la organización, ya que sólo se tiene el coste de la conexión a Internet en cada sede, pero presenta dos grandes inconvenientes:

- No se garantiza cierta calidad de servicio ni las prestaciones en las comunicaciones a través de Internet, por lo que sólo será válido para servicios que no tengan una gran dependencia del ancho de banda.

- No es seguro, ya que los datos viajan por redes compartidas en las que pueden ser interceptados, modificados, falsificados, etc.

Para paliar el segundo inconveniente, es necesario que los datos que se intercambian las organizaciones se cifren antes de enviarse por Internet, de forma que puedan ser descifrados al llegar a la sede destino. Esta funcionalidad, ofrecida por equipos dedicados en las redes privadas, es asumida por los cortafuegos que permiten definir reglas cuya acción es "Cifrar", en caso de que dicho tráfico sea destinado a las sedes remotas. De esta manera, se crean caminos seguros sobre Internet entre los cortafuegos de salida de cada una de las sedes, tal y como se ve en Figura 42.

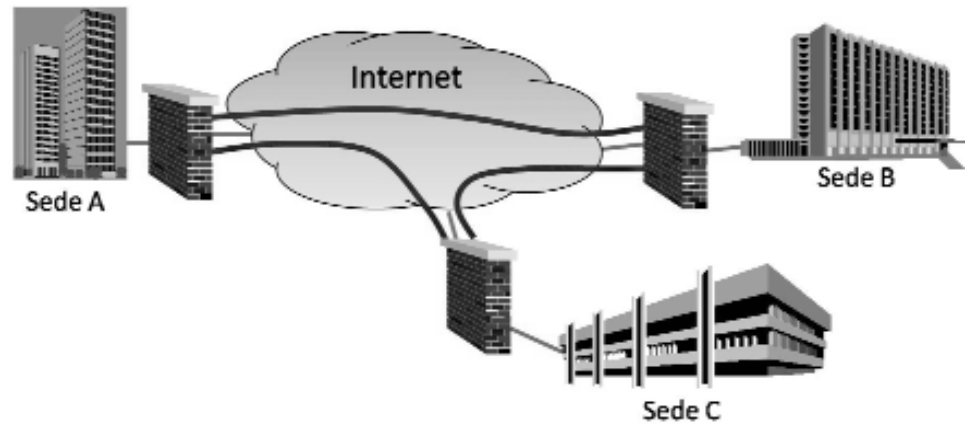

Figura 42: Redes Privadas Virtuales

El cifrado de las comunicaciones y el consiguiente descifrado exige una negociación previa entre los cortafuegos para la asignación de claves de cifrado, algoritmos, etc. Al principio, esta negociación se realizaba de una forma propietaria entre cortafuegos del mismo fabricante, por lo que las Redes Privadas Virtuales sólo se podían formar con los cortafuegos del mismo fabricante. Hoy existe una solución estándar para el cifrado de datos en tránsito que permite utilizar cortafuegos de distintos fabricantes para formar una Red Privada Virtual, basada en el protocolo IPSEC.

Las Redes Privadas Virtuales mostradas en la Figura 42, son denominadas también Redes Privadas Virtuales Estáticas, ya que los enlaces seguros entre cortafuegos son estáticos. Existe otro tipo de aplicación, orientada a la conexión de trabajadores remotos, conocida como Redes Privadas Virtuales bajo demanda, tal y como se muestra en la Figura 43.

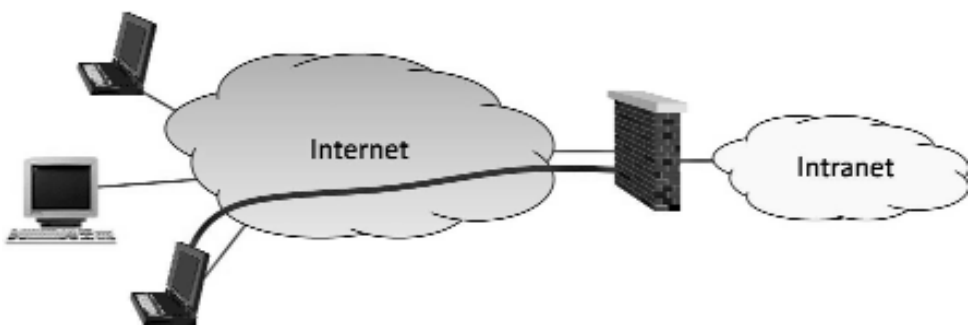

Figura 43: RPV bajo demanda

En este caso, los teletrabajadores quieren realizar una conexión remota a la red de la organización que debe ser protegida. Para ello, disponen de un software en su ordenador que es capaz de negociar con el cortafuegos de la organización el cifrado de los datos que se van a intercambiar sobre Internet. Nuevamente, esta funcionalidad que al principio era propietaria de los fabricantes de cada cortafuegos está normalizada ahora mediante el uso del protocolo IPSEC.

5.2.4.2 Traducción automática de direcciones

Otra funcionalidad adicional de los cortafuegos es la utilización de traducción automática de direcciones (*Network Address Translation-NAT*). Muchas organizaciones necesitan utilizar NAT por diversos motivos, como por ejemplo, el uso de direcciones privadas, confidencialidad del plan de direcciones interno, etc. En estos casos, se requiere un equipo específico que modifique las direcciones en la salida a Internet y que sea capaz de mantener tablas de correspondencia de direcciones en las conexiones establecidas.

Si la organización se protege del exterior con un cortafuegos de tipo pasarela de aplicación o de circuitos, la funcionalidad de NAT es innata a ellos, ya que la única dirección visible de la organización en Internet es la del interfaz externo del cortafuegos (el cortafuegos es el que establece las conexiones en estos casos con los destinos correspondientes). Pero si se tiene un cortafuegos de filtro de paquetes, es necesario incluir la funcionalidad de NAT en la salida a Internet. Por ello, muchos cortafuegos tienen ya incluida esta funcionalidad como parte de la política de reglas que se aplica a los datagramas de salida, pudiendo establecer distintas formas de asignación de direcciones.

5.2.4.3 Pasarela de aplicación transparente

Esta funcionalidad pretende combinar las ventajas de las dos principales tecnologías de cortafuegos:

- Los cortafuegos de tipo filtro de paquetes son transparentes para el usuario, que no tiene que modificar sus clientes o su configuración para atravesarlos. No se necesitan clientes específicos.

- Los cortafuegos de tipo pasarela de aplicación permiten el uso de la identidad del usuario como parámetro para establecer las configuraciones de seguridad, permitiendo reglas de seguridad mucho más específicas y concretas. Permiten filtrar por usuario.

La utilización de las pasarelas transparentes permite combinar ambas ventajas, a costa de "hacer trampas" en el uso de los protocolos de Internet. La Figura 44 muestra un ejemplo de uso de pasarela transparente.

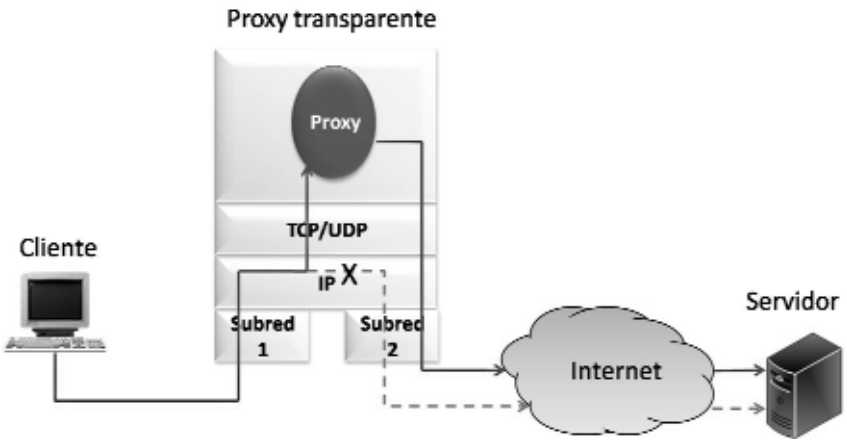

Figura 44: Pasarela transparente

Como se observa en la Figura 44, el cliente establece una conexión directamente hacia el servidor remoto. Cuando dicha conexión llega al cortafuegos, éste debería encaminarla hacia el destino a nivel IP, pero en vez de ello, el cortafuegos captura la conexión y la redirige hacia una pasarela servidora instalada en el propio cortafuegos. Esta pasarela analiza la conexión y en función de la configuración de seguridad puede optar por solicitar o no la identidad del usuario. En caso de elegir la opción de solicitar la identidad del usuario, la pasarela envía una respuesta a la conexión del cliente solicitándole su identidad, pero en lugar de utilizar como dirección de origen de la petición su propia dirección, la falsifica y la sustituye por la dirección IP del servidor remoto, puesto que el cliente espera una respuesta del servidor, no de ningún equipo intermediario.

El cliente, ante esta petición, enviará sus datos de identificación hacia el servidor, conexión que nuevamente será interceptada por el cortafuegos y redirigida a la pasarela transparente, que verificará la identidad del usuario y las reglas de acceso. Si la pasarela considera que la conexión debe ser aceptada, establecerá una conexión con el servidor solicitado y conectará ambas conexiones a nivel de aplicación, manteniendo la interceptación y redirección de las conexiones de salida, así como la sustitución de la dirección IP origen en las respuestas enviadas al cliente. De esta manera, se consigue el filtrado por identidad de usuario característico de las pasarelas de aplicación sin necesidad de modificar las aplicaciones de los clientes.

5.2.4.4 Seguridad en los contenidos

Los cortafuegos originales eran sistemas que utilizaban como parámetros de filtrado de tráfico las cabeceras de los protocolos de transporte y red, siendo en la mayoría de los casos suficiente para poder expresar las políticas de seguridad requeridas, ya que éstas se referían a los servicios en su totalidad (un servicio era aceptado o rechazado). Sin embargo, surgieron nuevos ataques basados en la utilización anormal de los servicios, atacando servidores Web con peticiones HTTP dañinas, o intercambiando virus a través de mensajería instantánea. Por ello, surgió la necesidad de diseñar las políticas de seguridad de tal forma que fueran capaces de discriminar por el contenido de los servicios, utilizando como parámetro de filtrado los campos de los protocolos de aplicación o incluso el propio contenido de los protocolos de aplicación. De esta manera, pueden ser detectados los contenidos maliciosos, improductivos, etc. Esto permite que el cortafuegos sea capaz de procesar no sólo las cabeceras de los protocolos de red y de transporte, sino también las de aplicación e incluso, en algunos casos, ser capaz de inspeccionar los contenidos del propio protocolo de aplicación.

Actualmente, el problema de la seguridad en los contenidos es de tal importancia que muchas veces es necesario disponer de un equipo específico que se encargue de tratarlo. No obstante, algunos cortafuegos también pueden llevar a cabo diversas tareas en este ámbito. Este tipo de cortafuegos son denominados frecuentemente cortafuegos con inspección profunda de paquetes (*Deep Packet Inspection*).

Se analizan a continuación los mecanismos de seguridad en contenidos específicos de tres tipos de servicios: conexiones Web, FTP y SMTP (correo electrónico).

Seguridad en las conexiones Web

Una de las principales causas que explican la necesidad de seguridad en los contenidos radica en la necesidad de filtrar las peticiones y respuestas del servicio de Web con el protocolo HTTP. Aunque, en teoría, el cortafuegos podría filtrar por cualquiera de los campos del protocolo HTTP, en la práctica el campo más importante es el filtrado por el URL solicitado en una petición, y por el contenido que se recibe en una respuesta.

El filtrado por URL permite a los administradores de seguridad expresar políticas de seguridad en las que se restrinja la conexión de los usuarios internos a determinados servidores Web que se consideren inapropiados, o en las que se autorice sólo conexiones a servidores Web autorizados. La

definición de estas políticas de configuración puede ser compleja dado el dinamismo y heterogeneidad de los servidores Web, y en muchos casos, la intención del administrador es bloquear un conjunto de servidores Web cuya temática o contenidos no se consideran apropiados. Por lo tanto, la configuración de seguridad para estos casos suele basarse en la definición de categorías de contenidos de servidores Web. El administrador restringirá o autorizará expresamente el acceso a servidores Web incluidos en unas categorías determinadas.

Una vez que el administrador ha definido las categorías, el problema se centra en cómo conocer que un determinado URL solicitado por un usuario, pertenece a una determinada categoría. La práctica más usual es el uso de categorizaciones de los contenidos de los servidores Web. Si un cortafuegos tiene definidas reglas para controlar el acceso a determinadas categorías de contenidos Web, cuando recibe una solicitud Web realizará una consulta al servidor de categorizaciones, el cual responderá con la categoría a la que pertenecen dichos contenidos. Esta información permitirá al cortafuegos aplicar la regla correspondiente en función de la categoría devuelta por el servidor. La comunicación entre el cortafuegos y estos servidores de categorización de contenidos es, en su gran mayoría, propietaria, aunque existen algunas propuestas para normalizar dichas solicitudes, como el denominado "URL *Filtering Protocol*" (UFP). Existen diversos métodos utilizados por estos servidores para categorizar el contenido:

- Uso de listas negras: lista de sitios con categorías ya predefinidas.

- Rastreo de contenido: utilización de algoritmos para deducir la categoría en función del contenido y de la aparición de palabras, frases, expresiones, etc.

Seguridad en las conexiones FTP

De una forma análoga a la seguridad en los contenidos Web, es posible configurar el cortafuegos para inspeccionar el tráfico que se está cargando o descargando a través de dicho cortafuegos. En este caso, la práctica más típica es la ejecución de programas antivirus a los archivos descargados, independientemente de su origen. Para ello, el cortafuegos puede incluir localmente un antivirus adaptado para su aplicación a tráfico en tránsito, o puede redireccionar este tráfico a un servidor especializado para que ejecute el antivirus. Este tipo de comunicación entre el cortafuegos y el servidor con el programa antivirus fue objeto de un intento de estandarización, en el denominado "*Content Vectoring Protocol*" (CVP).

Seguridad en las conexiones SMTP

Las conexiones de correo electrónico también pueden ser filtradas por el cortafuegos para controlar contenidos maliciosos o información confidencial. En este caso, los parámetros de filtrado pueden establecerse en función de los distintos campos de la cabecera o contenido del correo electrónico, tales como:

- Remitente.
- Destinatario.
- Análisis de veracidad de cabeceras.
- Análisis de SPAM del mensaje.
- Tamaño del mensaje.
- Tipo de anexos.
- Etc.

Las acciones que el cortafuegos puede llevar a cabo pueden ser:

- Reasignación del remitente para mensajes salientes.
- Reasignación del destinatario para mensajes entrantes.
- Eliminar anexos de un cierto tipo o tamaño.
- Descarte del mensaje.
- Modificación del *subject* para indicación de SPAM.
- Ocultación de campos del sobre para mensajes salientes.

Esta última acción (Ocultación de campos del sobre para mensajes salientes) puede ser muy útil en organizaciones en las que el correo saliente atraviesa diversos nodos de correos internos de la organización antes de enviarse al exterior. Todos estos nodos dejan una traza en la cabecera, trazas que luego podrían ser analizadas por los destinatarios para averiguar la estructura interna de la red de la organización. Los cortafuegos pueden ser configurados para dejar únicamente las trazas estrictamente necesarias.

Como se ha indicado anteriormente, una de las funciones que puede llevar a cabo un cortafuegos con el contenido del correo electrónico es la detección de SPAM o correo no deseado. Sin embargo, el volumen de SPAM existente y la complejidad que implica su detección debido a su constante evolución, hace que esta funcionalidad la realice un componente dedicado exclusivamente a ello, independientemente del cortafuegos.

5.3 Arquitectura de seguridad perimetral

Hasta ahora, el único elemento considerado para el control de acceso basado en defensa perimetral de una organización ha sido el cortafuegos. Es cierto que es el elemento más importante de una defensa perimetral, pero existen otro tipo de elementos que pueden cooperar en la defensa perimetral de la red de una organización, en solitario o de forma colaborativa entre ellos o con el cortafuegos. A continuación, se describen los más importantes.

5.3.1 Sistema de detección de intrusiones

Los Sistemas de Detección de Intrusiones, más conocidos como IDS (*Intrusion Detection Systems*), son sistemas que monitorizan los eventos que ocurren en sistemas, ordenadores y redes en busca de signos que revelen una posible intrusión, entendiendo como intrusión cualquier intento de comprometer alguna característica de los sistemas de una organización. Como resultado de esta monitorización, estos sistemas pueden proporcionar una información adicional al cortafuegos sobre las intrusiones o intentos de intrusiones existentes en la organización, que permite afinar y particularizar la configuración de seguridad.

Los IDS se pueden ubicar en distintos puntos de la organización:

- En el exterior de la red de la organización, sin protección del cortafuegos. En este caso, el IDS detectará múltiples intrusiones y comportamientos anómalos, que en principio deberán ser rechazados por el cortafuegos. La función de un IDS en este punto es complementar al cortafuegos para relacionar las intrusiones detectadas en el mismo IDS y las rechazadas por el cortafuegos, así como, en determinados casos, poder interaccionar con el cortafuegos ante algunos tipos de intrusiones que se produzcan en tráfico permitido por el cortafuegos.

- En la zona desmilitarizada de la red. Este es el punto más útil de ubicación de un IDS, ya que ese trata de la zona más desprotegida de la red que contiene activos a proteger. En esta zona, el IDS debe tener una sensibilidad alta ante los ataques, de forma que pueda interactuar con el cortafuegos rápidamente en caso de detección de intrusiones dirigidas hacia los equipos de la zona desmilitarizada.

- En la zona interna de la red. En esta zona, es necesario un IDS con la máxima sensibilidad, ya que cualquier identificación de intrusión supone máximo grado de alerta, al estar en la zona teóricamente protegida de la red, y es de vital importancia mitigarla.

Existen varios tipos de IDS, en función del punto de vista desde el que se analicen [25]:

- Según el tipo de fuentes de información que analiza.

- Según su frecuencia de tratamiento de eventos.

- Según sus principios de detección.

- Según su estrategia de control.

- Según sus acciones de respuesta.

Las próximas secciones detallan cada uno de estos tipos de IDS.

5.3.1.1 IDS según tipo de fuentes de información monitorizada

Según la información analizada por el IDS, se pueden distinguir cuatro tipos de IDS:

- HIDS (*Host-based IDS*), IDS de sistema: IDS que analiza información de un sistema (información de auditoría de actividades de usuario, información del sistema operativo, ficheros de sistema, ficheros de registro, etc.), en busca de indicios que denoten un comportamiento anómalo o cualquier otro signo de intrusión. El ejemplo más clásico de un IDS de sistema son los programas antivirus, que monitorizan el acceso a procesos dañinos, pudiendo incluso monitorizar la actividad del sistema operativo en busca de patrones sospechosos (intentos sospechosos de acceso a la libreta de direcciones, etc.). Estos sistemas permiten detectar ataques no visibles en la red, pueden trabajar en entornos con tráficos de red cifrados, no se ven afectados

por entornos de red basados en '*switch*' y tienen capacidad de detención de ataques interceptando llamadas al sistema o APIs conocidas. Sin embargo, en redes con muchos sistemas a proteger la gestión de los HIDS se vuelve muy compleja, al igual que el resto de aplicaciones del sistema son susceptibles de ser atacados, y presentan un coste de prestaciones y de espacio de almacenamiento de la máquina protegida.

- NIDS (*Network-based IDS*), IDS de red: IDS que analiza el tráfico de red que captura en segmentos de red de área local o enlaces troncales. Estos IDS suelen ser sistemas dedicados que escuchan constantemente todo el tráfico de la red, en modo promiscuo (es decir, escuchan todo el tráfico que circula por la red, aunque no esté dirigido hacia o generado por el propio sistema), intentando identificar patrones de tráfico que puedan ser caracterizados como intrusiones. Suelen necesitar varios sensores para monitorizar una gran red, siendo transparentes a la red e invisibles para los atacantes, y son sistemas muy seguros. Sin embargo, presentan dificultades para el procesamiento en redes con tráfico muy intenso. No obstante, se pueden mejorar con implementaciones hardware, a costa de reducir su capacidad de actualización.

- NNIDS (*Network-Node IDS*), IDS de nodo de red: este tipo de IDS es una variación de los NIDS anteriores, que analiza el tráfico dirigido hacia o generado por un único nodo. Usualmente, suele ser ejecutado en el propio nodo que protege por lo que no necesita escuchar en la red en modo promiscuo.

- AIDS (*Application-based IDS*), IDS de aplicación: este tipo de IDS es un subconjunto de los HIDS, basados en el análisis de información de una determinada aplicación y no en el análisis de todo el sistema, como ocurre en los HIDS. Están especializados en identificar intrusiones específicas de aplicación, como por ejemplo, intrusiones en servidores Web, bases de datos, etc. Estos IDS monitorizan la información de una aplicación concreta dentro de un sistema.

5.3.1.2IDS según frecuencia de tratamiento de eventos

Un IDS puede descomponerse en dos subsistemas: el sensor que monitoriza los eventos y el motor de análisis que analiza los eventos en busca de síntomas de intrusión. Según la relación que exista entre ambos módulos, en cuanto al tiempo transcurrido entre el momento en que ocurre el evento y el momento en que se produce su análisis, se distinguen dos modos de funcionamiento de los Sistemas de Detección de Intrusiones:

- Análisis periódico (*Batch Mode*): el flujo de información desde los sensores de monitorización hacia los motores de análisis no es continuo ('*store and forward*'). Esto permite menores requisitos de rendimiento del sistema, aunque no da opción a dar respuesta a la intrusión, ya que ésta es detectada bastante tiempo después de su aparición, lo que implica la posible consecución de la intrusión.

- Monitorización continua (Tiempo Real): los motores de análisis operan sobre una alimentación continua de información desde los sensores de monitorización. Es el modo de funcionamiento habitual en los NIDS, y permite detectar y tomar medidas durante el progreso del ataque, aunque implica mayores requisitos de rendimiento del sistema, lo que puede dar lugar a que sea imposible operar ante determinados volúmenes de información.

5.3.1.3IDS según principios de detección

Existen dos tecnologías principales que pueden ser utilizadas por el motor de análisis para detectar potenciales intrusiones:

- Detección de firmas: se basa en la búsqueda de patrones predefinidos que describen un ataque conocido. Se parte de bases de datos de firmas de ataques conocidos que pueden ser identificados al contrastar los eventos con los patrones de la base de datos. Esto hace que los IDS sean muy efectivos, es decir, que tengan muy pocos falsos positivos (se detecta como anómalo algo que no lo es), que permitan dar un diagnóstico rápido y fiable, y puedan incluso identificar el tipo y herramienta de ataque utilizadas. Sin embargo, este tipo de tecnologías presenta graves inconvenientes, ya que los IDS que la utilizan sólo detectan ataques conocidos, que han sido incorporados previamente a su base de datos de firmas. Esto hace que existan ventanas temporales de vulnerabilidad desde que surge el ataque hasta que éste es detectado e incorporado en una actualización de la base de datos de firmas, y que por tanto, aumente el número de

falsos negativos (se considera normal, comportamiento anómalo). Este tipo de sistema también falla ante pequeñas variaciones de ataques.

- Detección de anomalías: se basan en la identificación de comportamiento inusual en las fuentes de información (sistema o red). Los detectores de anomalías construyen perfiles de actividad NORMAL de usuarios, *hosts* y conexiones de red, a partir de datos históricos recogidos a lo largo de un período de operación normal, y contrastan la actividad existente en momentos concretos con el perfil histórico de actividad considerada normal, permitiendo detectar desviaciones significativas debidas a diversas causas, como la existencia de intrusiones. La principal ventaja de este tipo de detección es que produce muy pocos falsos negativos, ya que permite detectar un ataque sin conocimientos específicos previos acerca de él. Sin embargo, produce muchos falsos positivos y requiere un entrenamiento exhaustivo para que la generación de falsos positivos no haga inviable la utilización del IDS.

5.3.1.4 IDS según estrategia de control

En función de la interrelación entre distintos IDS dentro de las redes de la organización, existen dos tipos de estrategias de control que se pueden implementar:

- Estrategia centralizada: en esta estrategia, existen diversos sensores de monitorización en distintos puntos de la red, que envían los datos a un único motor de análisis, que es capaz de detectar intrusiones analizando los datos que recibe de todos los sensores. De esta forma, el motor de análisis puede relacionar información recibida de diversos sensores para realizar una detección más ajustada, o para descartar positivos falsos o duplicados. Todos los IDSs monitorizan datos, pero uno solo los analiza.

- Estrategia distribuida: se distribuyen tanto sensores de monitorización como motores de análisis, siendo cada IDS autónomo e independiente del resto de IDS, realizando tareas tanto de monitorización como de análisis.

5.3.1.5IDS según acciones de respuesta

Los IDS pueden caracterizarse igualmente según su capacidad de respuesta ante una intrusión. Si bien la tendencia actual es separar esta funcionalidad de la detección en los denominados Sistemas de Respuesta a Intrusiones (*IRS-Intrusion Response Systems*), en un principio los IDS podían asumir también ciertas acciones de respuesta. De esta forma, se pueden identificar distintos tipos de respuestas posibles a intrusiones:

- Respuestas reactivas: respuestas cuyo fin es proporcionar una solución o aviso tras la detección de una intrusión. Se dividen, a su vez, en dos grupos de respuestas:

  - Respuestas pasivas: acciones que se basan en avisar o informar de que se ha producido una intrusión o ataque en el sistema, pero no llevan a cabo ninguna acción para intentar mitigarlo. Son respuestas de registro, útiles para monitorización. Ejemplos de este tipo de respuestas son: registros normales/registros seguros (Canal de registro seguro); alertar a la consola central local y/o remota sobre posibles alertas detectadas; notificar al administrador o responsable de seguridad de la ocurrencia del ataque vía SMS, email, etc., TRAP, SNMP; activación del sistema de auditoría de una empresa u organización ante un acceso sospechoso; registrar las incidencias detectadas en una base de datos como evidencia de que algo no ha ido bien en el funcionamiento normal del sistema protegido; etc.

  - Respuestas activas: conjunto de acciones que tras detectar la intrusión, además de informar al administrador de la ocurrencia del ataque mediante notificación o alerta, llevan a cabo una acción de entre un conjunto de candidatos con el fin de mitigar el ataque o contrarrestarlo en el menor tiempo posible, sin necesidad de tener que informar al administrador y esperar a que este ejecute una respuesta. Es importante resaltar que, a pesar de que son las acciones más habituales, las respuestas que conlleven cualquier tipo de bloqueo suprimen toda interacción entre el atacante y el atacado. Otro problema de las acciones activas, y motivo por el cual son un campo activo de la investigación, es que las respuestas que se implementan hoy en día ignoran el coste que puede suponer una intrusión. De este modo, las respuestas podrían causar un daño mayor que las propias intrusiones.

A continuación se enumeran algunos ejemplos de los diferentes tipos de acciones activas incluidos en cuatro bloques distintos [26]:

- Respuestas de protección: bloquear sesión, o una dirección IP; cortar conexión TCP; reconfigurar cortafuegos (acceso), *router* (ACL), *firewall*, etc.; terminar el proceso sospechoso, desconectando al usuario dañino, modificando la lista de filtrado del *router*, o cerrando un servicio; reiniciar conexiones de *routers*, *firewall*, etc.; cerrar el sistema o un servicio; terminar, o reconfigurar una conexión de un *firewall* o de cualquier otro equipo del sistema; etc.

- Respuestas de recuperación: incrementar el nivel de sensibilidad de los sensores, notificando a los IDS, por ejemplo; restauración, es decir, devolver a un recurso atacado al estado en que se encontraba antes del ataque, a su estado anterior.

- Respuestas de decepción: si el destino final es un servidor Web alterno que personifica al original, este podría convertirse en un *Honeypot* transparente para el atacante y así realizar un estudio de éste; aislamiento del intruso, "*Fishbowl*"; sacrificio de recurso (siempre que sea un Recurso de *backup*).

- Respuestas de reacción: lanzar un contraataque; respuestas análogas al sistema nervioso autónomo; etc.

- Respuestas proactivas: este tipo de respuestas intentan evitar que ocurra el ataque, es decir, intentan detectar y contrarrestar el ataque antes de que cumpla su objetivo. Un ejemplo de ello sería, interrogar activamente a todos los procesos de usuario existentes utilizando identidades falsas Troyanas y terminar aquellos procesos que no se originaron de usuarios genuinos en lugares aprobados.

La Figura 45 muestra un esquema de clasificación de las posibles respuestas a intrusiones.

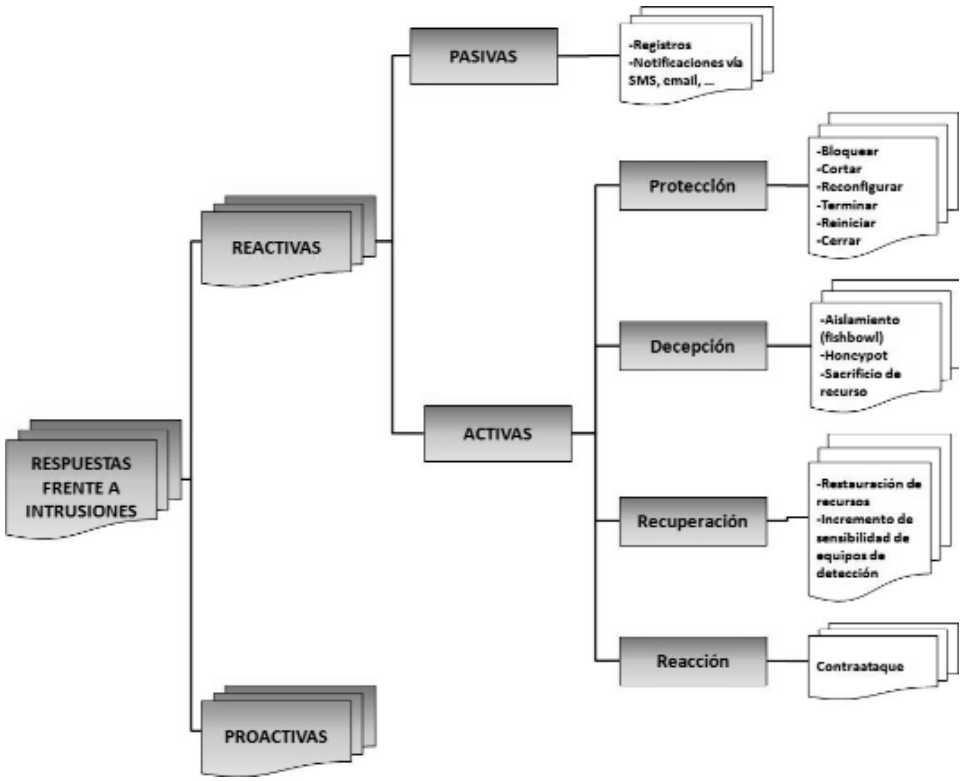

Figura 45: Catálogo de respuestas frente a intrusiones

No obstante, la mayoría de los IDSs son componentes pasivos, que sólo detectan las intrusiones e informan acerca de ello, es decir sólo llevan a cabo respuestas pasivas en la mayoría de los casos. Las reacciones a estas detecciones son responsabilidad de otros componentes denominados, Sistemas de Respuestas a Intrusiones (IRSs).

5.3.2 Señuelos (*Honeypots)*

Los señuelos, más conocidos por su denominación *honeypots* en inglés, son sistemas que se exponen voluntariamente en una organización como blanco de los ataques. Estos sistemas no están dentro del ámbito de protección normal de la arquitectura de seguridad de la organización, ni se les aplican todas las medidas de seguridad normales del resto de los sistemas de la organización.

Aunque pueda parecer paradójico intentar atraer a los atacantes a la organización a través de estos señuelos, su utilización tiene varias ventajas:

- Es posible aprender las técnicas de los atacantes, lo que permite mejorar la defensa de los sistemas de la organización. Como ya dijo el general chino Sun Tzu en su obra "El arte de la guerra" en el siglo VI a. C., una de las mejores armas para combatir es "conocer a tu enemigo". El uso de señuelos de una forma controlada y vigilada permite conocer cuáles son las técnicas del enemigo y ajustar y afinar las tecnologías de defensa con dichos conocimientos.

- La utilización de señuelos permite que el atacante "pierda el tiempo" con estos sistemas antes de llegar a otros sistemas más relevantes para la organización. Por ello, es posible detectar la presencia del atacante en estos señuelos y de esta forma tomar las medidas preventivas necesarias para evitar el progreso del atacante al resto de las redes de la organización.

Los señuelos son sistemas extremadamente sensibles, y hay que tener grandes precauciones en cuanto a su configuración:

- Deben estar aislados de la red de la organización. En ningún caso debe existir una vía de acceso desde los señuelos a los sistemas de la organización, ya que el atacante puede ser capaz de encontrarlos y acceder de forma rápida a ellos.

- Deben aparentar ser sistemas normales, es decir, deben incluir vulnerabilidades suficientes para que el atacante pueda explotarlas, aunque éstas no deben ser tan obvias como para que el atacante pueda sospechar que se trata de un señuelo.

- Deben permitir el registro totalmente transparente de la actividad de los atacantes, sin que pueda ser detectado por ellos, de forma que se pueda analizar y aprender posteriormente de la actividad de los atacantes.

- No pueden incluir ningún tipo de información importante o sensible de la organización, como nombres de usuarios o claves reales.

- Deben ser fácilmente recuperables y reemplazables ante una destrucción del sistema.

Para el despliegue de señuelos, existen dos alternativas:

- Las denominadas cajas de sacrificio, que son sistemas absolutamente normales que incluyen vulnerabilidades, y que se ponen a disposición del atacante. Estos sistemas tienen un canal de registro seguro e indetectable para grabar toda la actividad del atacante de una forma transparente. Son sistemas de usar y tirar que deben ser reemplazados tras cada ataque por otro nuevo.

- Sistemas emulados, que permiten emular la presencia de servidores con vulnerabilidades y reaccionar a las secuencias de ataques típicas de los atacantes, haciéndoles creer que están ante un sistema real. Estos sistemas tienen la desventaja de que se restringen al ataque a un cierto servidor, sin poder aprender acciones más allá del propio servidor atacado.

Es fundamental en el despliegue de señuelos que éstos sean lo más veraces posibles para no provocar desconfianza en el atacante. Por ello, muchas veces no es recomendable poner un único sistema señuelo aislado, ya que no es una situación normal en una organización, lo que puede dar lugar a sospechas. Por este motivo, surge el concepto de Redes Señuelo (*Honeynet)* [27] en las que existen diversos señuelos conectados en red, incluyendo incluso *routers* señuelo. Este tipo de infraestructura es más costoso ya que es necesario montar una red y múltiples sistemas dedicados exclusivamente a ser atacados, pero a cambio, se obtiene una visión más real de la organización que va a permitir atraer a más atacantes, y lo que es más importante, se pueden tener múltiples señuelos heterogéneos de forma que se aprenda sobre los ataques a distintos entornos y servicios (Windows, Linux, *routers*, etc.) simultáneamente. Una alternativa para el despliegue de redes señuelo de una forma sencilla y barata es la utilización de sistemas en red virtualizados, de forma que sobre una única máquina anfitriona se puedan desplegar diversos sistemas virtualizados conectados en red. Es especialmente importante en este caso, esconder los síntomas de virtualización, para que el atacante no pueda detectarlos y de esta forma evitar sospechas.

5.3.3 Inspectores de contenidos

Como se ha visto anteriormente, los cortafuegos han ido adquiriendo con el paso del tiempo funcionalidades que pueden sobrecargar a estos equipos. En especial, las funcionalidades de filtrado en función de los contenidos de los paquetes resultan muy pesadas y pueden derivar en problemas en las prestaciones del cortafuegos. Por ello, en los últimos años han aparecido equipos especializados en este tipo de tareas, pudiendo reducir de esta forma la carga del cortafuegos. Son los denominados inspectores de contenidos, que se encargan de garantizar la política de seguridad de la organización en cuanto a los contenidos del tráfico saliente y entrante. Estos equipos se encargan de aplicar políticas de filtrado para diferente tipo de contenidos:

- Acceso saliente a servidores Web, estableciendo filtros en función de la categoría de los contenidos de los servidores Web.

- Acceso saliente de mensajes de correo electrónico, estableciendo filtros para impedir la transmisión de información sensible, como cabeceras con información sobre la red interna, o análisis de documentos anexos, etc.

- Acceso entrante de mensajes de correo electrónico, con tecnología específica para detectar correo electrónico no deseado y capacidad de aplicar filtrado en función de ello.

- Acceso entrante de contenidos, para detectar la entrada de contenidos de los denominados "*malware*", como virus, troyanos, programas espías, etc.

5.3.4 Seguridad en los bastiones

Otro aspecto muy importante que refuerza la arquitectura de seguridad de una organización es asegurar al máximo los equipos que albergan servidores públicos, también denominados bastiones. Estos equipos albergan servicios que no pueden ser protegidos por el cortafuegos, como los servidores Web, correo electrónico o DNS, lo que los convierte en un potencial punto de acceso de los atacantes a la red, por lo que deben ser protegidos al máximo. Por tanto, resulta imprescindible cuidar la seguridad de estos sistemas, con un conjunto de medidas:

- Instalar un Sistema Operativo de confianza, con los últimos parches de seguridad y con todas las actualizaciones disponibles.

- Estos sistemas no deben contener información sensible, como documentos o cuentas de usuario.

- Deben proporcionar sólo los servicios estrictamente necesarios, eliminando cualquier servicio de red que no sea esencial.

- Deben estar protegidos con un cortafuegos personal que permita el acceso sólo a los servicios proporcionados.

- Deben estar preparados para posibles desastres, manteniendo copias de seguridad muy frecuentes, y salvaguardando los registros del sistema en almacenamiento externo.

- Deben utilizarse programas de auditoría de seguridad periódicamente, que permitan detectar modificaciones no deseadas en programas y procesos del sistema.

5.3.5 Otros

Aparte de los sistemas expuestos, existen otros elementos que pueden ayudar a mejorar la arquitectura de seguridad del sistema, como sistemas de captura de tráfico que analizan el tráfico en segmentos de red sensibles, o sistemas detectores de sondas que permiten detectar a usuarios internos que están escuchando el tráfico de la red, etc.

Capítulo 6

Catálogo de empresas e instituciones de seguridad en red

6.1 Empresas nacionales

En el campo de la seguridad en red, existen muchas empresas españolas dedicadas a diversos aspectos de la seguridad en red, desde distintos puntos de vista: desarrolladoras de software de seguridad en red, fabricantes de equipos de seguridad en red, empresas que ofrecen soluciones de integración de seguridad y empresas que se especializan en la consultoría y auditoría de seguridad en red. Existen también empresas que tienen un espectro de actividad mucho mayor (por ejemplo, INDRA o Telefónica I+D), proporcionando soluciones tecnológicas muy amplias entre las que se incluyen sistemas de seguridad en red. La siguiente lista detalla las empresas españolas más especializadas en el área de la seguridad en red, en el ámbito del desarrollo de software específico o equipos especializados [28].

ACOTEC

- URL: www.acotec.es
- E-mail: acotec@acotec.es
- Dirección: Parque Tecnológico de Castilla Y León. c/ Juan Herrera, 16. Edificio Centro, Módulos 211-213. 47151 Boecillo (Valladolid).
- Uso de tarjetas inteligentes como llave de seguridad: autenticación e identificación, firma electrónica, monedero electrónico, etc.

ADICIONA

- URL: www.adiciona.com
- E-mail: adiciona@adiciona.com
- Dirección: avda. Meridiana 358, 8º AB. 08027 Barcelona.
- Filtro de correo electrónico saliente.

C3PO

- URL: www.c3po.es
- E-mail: c3po@c3po.es
- Dirección: c/ Alejandro Goicoechea, 6. 08960 St. Just Desvern (Barcelona).
- Tarjetas inteligentes, dispositivos biométricos, firma electrónica.

GMV

- URL: www.gmv.es
- E-mail: marketing-GMV-SGI@gmv.com
- Dirección: c/ Isaac Newton, 11 P.T.M. 28760 Tres Cantos (Madrid).
- Sistemas de gestión de seguridad de la información.

GRUPOICA

- URL: www.grupoica.com
- E-mail: info@grupoica.com
- Dirección: c/ Alejandro Rodríguez, 32. 28039 Madrid.
- Sistemas de gestión de seguridad de la información.

HISPASEC

- URL: www.hispasec.com
- E-mail: info@hispasec.com
- Dirección: avda Juan López Peñalver, 17. Edificio Centro de Empresas CEPTA, planta 3. Parque Tecnológico de Andalucía. 29590 Campanillas (Málaga).
- Alerta de vulnerabilidades.

ICAR VISION SYSTEMS

- URL: www.icarvision.com
- E-mail: icar@icarvision.com
- Dirección: c/ Ronda Can Fatjó, 21. Parc Tecnològic del Vallès. 08290 Cerdanyola del Vallès (Barcelona).
- Sistemas de control de acceso.

IDONEUM

- URL: www.idoneum.net

- E-mail: idoneum@idoneum.net

- Dirección: Polígono Industrial Pla d'en Coll. c/ Fresser, 12 C. 08110 Montcada i Reixac (Barcelona).

- Control de acceso basado en tarjetas.

IKUSI

- URL: www.ikusi.com

- E-mail: ikusi@ikusi.com

- Dirección: Paseo Miramón, 170. 20009 San Sebastián.

- Control de acceso físico.

INDENOVA

- URL: www.indenova.com

- E-mail: indenova@indenova.com

- Dirección: c/ Dels Traginers, 14 2ªB. Polígono Vara de Quart. Edificio Imper. 46014 Valencia.

- Firma electrónica.

INTELLIGENT DATA

- URL: www.intelligentdata.es

- E-mail: info@intelligentdata.es

- Dirección: Edificio InverInnova. avda. Punto Movi, 4 - TECNOALCALÁ. 28805 Alcalá de Henares (Madrid).

- Soluciones de control de acceso.

IPSCA

- URL: www.ipsca.com
- E-mail: general@ipsca.com
- Dirección: Edificio Twin Golf A. c/ Perú, 6. 28290 Las Rozas (Madrid).
- Sistemas de firma electrónica.

IRONGATE

- URL: www.iron-gate.net
- E-mail: info@iron-gate.net
- Dirección: c/ Hermanos García Noblejas, 39-5º. 28037 Madrid.
- Sistemas de defensa perimetral.

ISDEFE

- URL: www.isdefe.es
- E-mail: general@isdefe.es
- Dirección: c/ Edison, 4. 28006 Madrid.
- Sistemas de gestión de seguridad de la información.

IZENPE

- URL: www.izenpe.com
- E-mail: info@izenpe.com
- Dirección: c/ Beato Tomás de Zumárraga, 71 - 1º. 01008 Vitoria-Gasteiz.
- Sistemas de firma electrónica.

KABEL

- URL: www.kabel.es
- E-mail: info@kabel.es
- Dirección: c/ Foronda, 4-2ª planta. 28034 Madrid.
- Sistemas de control de acceso y gestión unificada de amenazas.

KSI Seguridad Digital

- URL: www.ksitdigital.com
- E-mail: info@ksitdigital.com
- Dirección: c/ Pío XII, 31-Entreplanta izqda - 31008 Pamplona.
- Sistemas de firma electrónica y cifrado.

MOSSEC

- URL: www.mossec.com
- E-mail: info@mossec.com
- Dirección: Ctra. Zaragoza N-330, Km.566. Parque Tecnológico Walqa. Edificio Félix Azara. 22197 Cuarte (Huesca).
- Seguridad en dispositivos móviles.

NETSIGNIA

- URL: www.netsignia.es
- E-mail: netsignia@netsignia.es
- Dirección: c/ Alcalá 117, bajo izqda. Madrid.
- Sistemas de control de acceso.

OPENWIRED

- URL: www.openwired.net
- E-mail: info@openwired.net
- Dirección: c/ Caballero, 87, bajo. 08029 Barcelona.
- Sistemas IPS.

OPTENET

- URL: www.optenet.com
- Dirección: c/ José Echegaray, 8. Edificio 3, 1ª Planta, módulo 1. Parque empresarial Alvia. 28230 Las Rozas (Madrid).
- Sistemas de filtrado de contenidos.

OZONO SECURITY

- URL: www.ozonosecurity.com
- E-mail: info@ozonosecurity.com
- Dirección: Plza. Poeta Vicente Gaos, 3, Bajo. 46021 Valencia.
- Protección de sistemas.

PANDA SECURITY

- URL: www.pandasecurity.com
- E-mail: info@es.pandasecurity.com
- Dirección: c/ Ronda de Poniente, 17. 28760 Tres Cantos (Madrid).
- Protección de sistemas.

REALSEC

- URL: www.realsec.com
- E-mail: info@realsec.com
- Dirección: c/ Orense, 68-11. 28020 Madrid.
- Sistemas de firma digital y cifrado.

S21SEC

- URL: www.s21sec.com
- E-mail: info@s21sec.com
- Dirección: Parque empresarial La Muga, 11. 31160 Orcoyen (Navarra).
- Sistemas de gestión de vulnerabilidades, gestión de eventos, IDS, IPS.

SAFELAYER

- URL: www.safelayer.com
- E-mail: sflyr@safelayer.com
- Dirección: Edif. World Trade Center. Edif. Sur Planta 4ª Moll de Barcelona s/n. 08039 Barcelona.
- Identificación electrónica, firma electrónica, PKI.

SAGE SP

- URL: www.sage.es
- E-mail: info@sage.es
- Dirección: c/ Labastida, 10-12. 28034 Madrid.
- Sistema antivirus.

SECUWARE

- URL: www.secuware.com
- E-mail: info@secuware.com
- Dirección: Plaza Ruiz Picasso, s/n. Torre Picasso, Planta 14. 28020 Madrid.
- Gestión de identidades y accesos, protección de la información, políticas de seguridad.

SEGLAN

- URL: www.seglan.com
- E-mail: info@seglan.com
- Dirección: c/ Antonio de Cabezón, 83. 28034 Madrid.
- Servicios y soluciones de pago, autenticación robusta, movilidad y firma.

SMART ACCESS

- URL: www.smartaccess.es
- E-mail: info@smartaccess.es
- Dirección: Paseo de la Castellana, 129. 28046 Madrid.
- Sistemas de control de acceso.

SPAMINA

- URL: www.spamina.com
- E-mail: info@spamina.com
- Dirección: c/ Constitució, 3, 5º 6ª. 08960 Sant Just Desvern (Barcelona).
- Sistema de control de SPAM y contenidos.

TOTEM GUARD

- URL: www.totemguard.es
- E-mail: comercial@totemguard.es
- Dirección: avda. Diagonal, 508-3º 4ª. 08006 Barcelona.
- Gestión de seguridad de equipos y servidores.

XIFRA

- URL: www.xifra.es
- E-mail: clientes@xifra.es
- Dirección: c/ Valencia, 40 - 4ª planta. 08015 Barcelona.
- Sistemas de defensa perimetral.

ZITRALIA

- URL: www.zitralia.com
- E-mail: info@zitralia.com
- Dirección: Ctra. Zaragoza N-330, Km.566. Parque Tecnológico Walqa, Ed.2. 22197 Cuarte (Huesca).
- Cifrado, seguridad en accesos remotos.

6.2 Empresas internacionales

Dado el gran número de empresas internacionales, se muestra a continuación una selección de las más representativas en el ámbito de la seguridad en red.

Fabricantes de cortafuegos de red

- Novell: Bordermanager.
- Borderware: Borderware Steelgate.
- Cisco: CISCO ASA.
- SecureComputing: Sidewinder.
- Cyberoam: Gateway Security Appliance.
- Checkpoint: Firewall-1.
- GNATBox: GB-Ware.
- Hewlett Packer: HP ProCurve.
- eSoft: Instagate.
- Alcatel-Lucent: Firewall Brick.
- SonicWall: Network Security Appliances.
- BizGuardian: BizGuardian Firewall.
- Juniper: Netscreen.
- Microsoft: ISA Server.
- Stonesoft: Stonegate.
- WatchGuard: Firebox.
- NetASQ: U series.

Fabricantes de cortafuegos personales

- Sunbelt: Sunbel Personal Firewall.
- Tallemu: Online-Armor.
- Comodo: Personal Firewall Pro.
- Computer Associates: CA Personal Firewall.
- Microsoft: Microsoft Windows Firewall.
- Looknstop: looknstop Firewall.
- NTKernel: NeT Firewall.
- Agnitum: Outpost Firewall.
- Preventon: Personal Firewall.
- Privacyware: Private Firewall.
- Deerfield: Visnetic Firewall.
- Lavasoft: Lavasoft Personal Firewall.

Los siguientes fabricantes ofrecen soluciones de cortafuegos personales integradas en suites de seguridad personal que combinan antivirus, antispam, *detectors de malware*, etc.

- Checkpoint: ZoneAlarm internet Security.
- Bullguard: Bullguard Internet Security.
- F-Secure: Internet Security.
- Kaspersky: Internet Security.
- McAfee: Total Protection.
- Symantec: Norton Internet Security.
- Panda: Panda Security (fabricante español).
- Trend Micro: Trend Micro Internet Security.

Fabricantes de soluciones de autenticación y *Single Sign On*

- 2AB: iLock Access Decision.
- Authenex: Authenex Strong Authentication System (ASAS).
- Cafesoft: CAMS.
- Computer Associates: CA Access Control.
- Entegrity: Entegrity Secure Access.
- Entrust: Entrust Security Manager.
- Evidian: IAM Suite.
- Hitachi: Identity Management Solutions.
- Novell: Novell Identity Manager.
- Oracle: Oracle Identity Management.
- ActivIdentity: ActivIdentity SecureLogin SSO.
- RSA: SecurID, Authentication manager.
- Sun: Sun OpenSSO Enterprise.
- IBM: Tivoli Identity manager.

6.3 Asociaciones empresariales y fundaciones en España

Existen diversas asociaciones empresariales en España desde las cuales se fomentan y promueven diversas actividades en el ámbito de la seguridad en red. Las más significativas en este ámbito son:

AETIC

Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España, resultado de la fusión de la Asociación Nacional de Industrias Electrónicas y de Telecomunicaciones (ANIEL) y la Asociación Española de Empresas de Tecnologías de la Información (SEDISI).

AETIC representa a cerca de 1.000 asociados, de los cuales 300 son empresas individuales y el resto de grupos y colectivos empresariales, cuya actividad está relacionada con la Electrónica, las Tecnologías de la Información y las Telecomunicaciones.

AETIC quiere promover el desarrollo del sector de la Electrónica, las Tecnologías de la Información y las Telecomunicaciones, especialmente con la generación de valor añadido y de actividad industrial o de servicios. Además, AETIC quiere potenciar el desarrollo de la Sociedad de la Información en España y apoyar la oferta empresarial en las áreas que representa.

Impulsada por esta asociación, se ha creado eSEC, Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza. Nació en el 2005 a iniciativa de la industria sectorial y con el apoyo de Ministerio de Industria, Turismo y Comercio, Ministerio de Educación y Ciencia y CDTI. Esta plataforma es una red de cooperación científico-tecnológica en cuyo seno se agrupan entidades de muy distinta naturaleza, pero principalmente empresas (grandes y PYMEs) y organismos de investigación (centros tecnológicos, Universidades y OPIs), interesadas en el sector de la seguridad y confianza.

Los objetivos principales de esta plataforma son:

- Definir una Agenda Estratégica de Investigación donde se incluyan las prioridades de I+D+i del subsector de Seguridad y Confianza.

- Movilizar la masa crítica de investigación, desarrollo y esfuerzo innovador necesarios para dar un empuje al subsector español de de Seguridad y Confianza tanto a nivel nacional como europeo mediante el fomento de la cooperación y la generación de proyectos.

Los miembros de la plataforma están organizados en torno a grupos de trabajo temático, entre los que se incluyen algunos muy relacionados con el área específica de Seguridad en Red:

- Identificación y control

- Seguridad de infraestructuras

- Gestión de la e-Identidad y la e-Reputación

ASIMELEC

ASIMELEC es la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones fundada en 1984, agrupa a fabricantes, comercializadores y en el caso del sector de las Telecomunicaciones a instaladores de productos de electrónica en sus diversas áreas.

ASIMELEC surge con el fin de defender y representar los intereses comunes de las empresas del sector. Por esta razón, entre las actividades que desarrolla se encuentra el establecimiento de una vía de comunicación con la Administración española y comunitaria representando a los distintos sectores que componen la asociación. Al mismo tiempo, participa en diferentes instituciones, tanto nacionales como europeas, lo que permite conocer la evolución del sector y transmitir los intereses de las empresas asociadas. Por otro lado, y para facilitar la consecución de los mismos objetivos, las empresas asociadas constituyen comisiones o grupos de trabajo, lo que les permite llevar a cabo acciones de promoción, solución de problemas comunes, análisis de normativa, etc.

Actualmente ASIMELEC cuenta con más de 2000 empresas representadas en la asociación, las cuales generan una facturación del 3% del PIB español. Las empresas asociadas a ASIMELEC se reúnen formando comisiones o grupos de trabajo en las que se analiza la problemática de su mercado, se realizan acciones conjuntas: estudios de mercado, elaboración de informes, realización de campañas de comunicación, organización de jornadas técnicas, solución a problemas comunes a las empresas del sector, estadísticas del sector, etc. Entre estas comisiones, destaca para el ámbito de este cuaderno la Comisión de Seguridad en las Tecnologías de la Información y Confianza en la Red, la cual agrupa los intereses de cuarenta y dos empresas de los diferentes sectores de la seguridad TIC. Su misión principal es la mejora de la confianza y seguridad en la sociedad de la información y su objetivo se centra en concienciar y promover el uso de las tecnologías de seguridad de los sistemas de información ante los usuarios, administración y opinión pública en general.

En la comisión están constituidos seis grupos de trabajo internos: marketing y comunicación, legislación, common-criteria, e-DNI, PSC y técnico. Además, dependen de ella los grupos multisectoriales de e-FACTURA, e-DNI e identidad digital

Sus actividades anuales, además de las reuniones de sus grupos, incluyen los Congresos de Identidad Digital y de Factura Electrónica, jornadas en distintas CC.AA., máster en Dirección de Seguridad de las TI con la Universidad Politécnica de Madrid y máster de e-gobernanza con IT DEUSTO, así como el impulso de proyectos dentro de los programas PROFIT, ARTEPYME, AVANZA, etc.

AFARMADE

AFARMADE es la Asociación Española de Fabricantes de Armamento y Material de Defensa y Seguridad. Se define como una asociación profesional, privada, de carácter empresarial, sin ánimo de lucro, que tiene por objeto la defensa y fomento de los intereses comunes de los fabricantes españoles de armamento y material de defensa y seguridad. AFARMADE es un foro de encuentro entre empresas y Administración, donde se expone y discute la problemática del sector, al mismo tiempo que constituye una importante plataforma para la defensa de los intereses de las empresas involucradas en defensa, tecnología de doble uso y seguridad.

Para el mejor cumplimiento de sus fines, AFARMADE se mantiene en contacto permanente con la Administración pública española y con asociaciones y entidades similares de otros países, o de carácter supranacional.

Como asociación profesional, AFARMADE está integrada por empresas españolas, públicas o privadas, relacionadas con la fabricación y tecnología del material de defensa y seguridad, agrupadas en los siguientes subsectores:

- Armamento y munición.
- Plataformas terrestres.
- Plataformas navales.
- Aeroespacial.
- Electrónica, comunicaciones, óptica, e informática.
- Ingeniería e I+D.
- Material de seguridad y equipamiento especializado.

En las áreas de electrónica, comunicaciones, óptica, e informática e Ingeniería e I+D se realizan y promueven actividades relacionadas con el ámbito de la Seguridad en Redes de Comunicaciones, en las líneas de promoción exterior de las empresas del sector, elaboración de informes y estudios y organización de cursos, jornadas y foros.

FUNDACIÓN CÍRCULO DE TECNOLOGÍAS PARA LA DEFENSA Y LA SEGURIDAD

La Fundación Círculo de Tecnologías para la Defensa y la Seguridad está constituida como lugar de encuentro para el intercambio de información entre todas las personas y entidades relacionadas con el sector de las tecnologías para la defensa y la seguridad. Con origen en el Círculo de Electrónica Militar, ha evolucionado en los últimos años abriendo el campo de actuación a las tecnologías para la defensa y la seguridad.

Sus objetivos principales son:

- Fomento de iniciativas que tiendan a la creación y el desarrollo de una tecnología nacional de aplicación a la defensa y la seguridad, especialmente en las áreas de electrónica, informática y comunicaciones.

- Actuar de catalizador en las relaciones entre personas, organismos y empresas que tienen intereses y realizan actividades dentro del sector de la defensa y la seguridad.

- Facilitar a los asociados una permanente actualización de las tecnologías de la defensa y la seguridad a través de actividades de formación, investigación y desarrollo.

Entre sus actividades se incluyen la organización de diversas jornadas y mesas redondas sobre temas específicos relacionados con la defensa y la seguridad, cursos de formación, reciclaje y especialización sobre tecnologías avanzadas (máster en Sistemas de Comunicación e Información para la Seguridad y la Defensa de la Universidad Politécnica de Madrid), elaboración de estudios e informes sobre la situación de la industria en el sector, etc.

6.4 Organismos de investigación en España

INTECO

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), promovido por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

INTECO tiene un doble objetivo: contribuir a la convergencia de España con Europa en la Sociedad de la Información y promover el desarrollo regional, enraizando en León un proyecto con vocación global. Desarrolla, entre otras, iniciativas de seguridad tecnológica, accesibilidad e inclusión en la sociedad digital y soluciones de comunicación para particulares y empresas. La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano.

Actualmente, INTECO tiene cuatro grandes programas: Seguridad, Accesibilidad, Calidad del Software y TV Interactiva. Dentro del programa de Seguridad, se desarrollan los siguientes proyectos en el ámbito de la seguridad tecnológica orientados a prestar servicio a ciudadanos y PyMEs:

- Centro de Respuesta a Incidentes en Tecnologías de la Información para PyMEs y Ciudadanos: sirve de apoyo al desarrollo del tejido industrial nacional y ofrece los servicios clásicos de un centro de respuesta a incidentes, dando soluciones reactivas a incidentes informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad a la PYME y ciudadanos españoles.

- Observatorio de la Seguridad de la Información: tiene como misión principal la de analizar, describir, asesorar y difundir la cultura de la seguridad y la confianza en la Sociedad de la Información, mediante la generación de conocimiento especializado en la materia, y la elaboración de recomendaciones y propuestas que permitan definir tendencias válidas para la toma de decisiones en el ámbito de la seguridad.

- Centro Demostrador de Seguridad para la PyME: tiene como misión principal potenciar el uso de las tecnologías relacionadas con la seguridad en las PyMEs españolas, para ello, proporcionará un catálogo de soluciones de seguridad informática que ayude a cubrir sus necesidades y apoyar su desarrollo.

INTA

El INTA (Instituto Nacional de Técnica Aeroespacial) es un organismo público de investigación especializado en la investigación y desarrollo tecnológico aeroespacial.

Entre sus principales funciones cabe destacar:

- La adquisición, mantenimiento y mejora continuada de todas aquellas tecnologías de aplicación en el ámbito aeroespacial.

- La realización de todo tipo de ensayos para comprobar y certificar materiales, componentes, equipos, subsistemas y sistemas de aplicación en el campo aeroespacial.

- El asesoramiento técnico y la prestación de servicios a entidades y organismos oficiales, así como a empresas industriales o tecnológicas.

- La actuación como centro tecnológico del Ministerio de Defensa.

La actividad científico-técnica del Instituto se articula en torno a un centenar de proyectos de investigación. Más de la mitad de los recursos económicos del INTA se destina a la realización de actividades de desarrollo tecnológico, una tercera parte a investigaciones aplicadas, y el resto a acciones de investigación básica.

Para el desarrollo de sus actividades el INTA se estructura en torno a departamentos y centros que, dependiendo de sus competencias propias, pueden agruparse en dos grandes áreas:

- Investigación + Desarrollo + Innovación (I+D+i)

- Certificación y ensayos.

Uno de los centros del INTA relacionado con el ámbito de este cuaderno es el Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI). Este centro evalúa la seguridad de las tecnologías de la información (TICs) de acuerdo a estándares internacionales reconocidos (ISO 15.408/Common Criteria, ITSEC y la ley española de firma electrónica) operando dentro del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TICs y del Centro Criptológico Nacional.

CNI

El Centro Nacional de Inteligencia (CNI) es el organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

Dentro del CNI se encuadra el Centro Criptológico Nacional (CCN), organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra y de garantizar la seguridad de las tecnologías de la información en ese ámbito. La Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) es tan importante para la seguridad y el bienestar de los ciudadanos como lo es la protección de los propios ciudadanos, sus intereses y su sociedad. Por tanto, se hace necesaria la existencia de este organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de los productos y de los sistemas de las TIC.

El ámbito de actuación del Centro Criptológico Nacional comprende:

- La seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.

- La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada.

Dentro de su ámbito de actuación, el Centro Criptológico Nacional realizará las siguientes funciones:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

- Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

- Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

- Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas.

- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países.

CSIC

El Consejo Superior de Investigaciones Científicas (CSIC) es una agencia estatal que constituye el Organismo Público de Investigación más importante de España. Con implantación en todas las Comunidades Autónomas a través de 126 centros y 145 unidades asociadas.

El objeto del CSIC es el fomento, la coordinación, el desarrollo y la difusión de la investigación científica y tecnológica, de carácter multidisciplinar, con el fin de contribuir al avance del conocimiento y al desarrollo económico, social y cultural. Además se ocupa de la formación de personal y del asesoramiento a entidades públicas y privadas en estas materias.

Entre sus funciones, destacan las siguientes:

- Realizar investigación científica y tecnológica y, en su caso, contribuir a su fomento.

- Transferir los resultados de la investigación científica y tecnológica a instituciones públicas y privadas.

- Proporcionar servicios científico-técnicos a la Administración General del Estado así como a otras Administraciones e instituciones públicas y privadas.

- Impulsar la creación de entidades y empresas de base tecnológica.

- Contribuir a la creación de entidades competentes para la gestión de la transferencia y la valoración de la tecnología.

- Formar investigadores.

- Formar expertos a través de cursos de alta especialización.

- Fomentar la cultura científica en la sociedad.

Se organiza en ocho áreas científico-técnicas, en las que se incluye el área de Ciencia y Tecnologías Físicas, en las que existen diversos centros e institutos relacionados con el área de Seguridad en Red. En concreto, el Instituto de Física Aplicada (IFA) cuenta con el Departamento de Tratamiento de la Información y Codificación, en el que se integra un Grupo de Investigación en Criptología y Seguridad de la Información, con actividad en:

- Estudio matemático de los códigos secretos o criptosistemas; que comprende la criptografía, o arte del diseño de criptosistemas y el criptoanálisis, o arte de la rotura de estos.

- La gestión del riesgo de los sistemas informáticos, mediante la evaluación de vulnerabilidades, identificación de amenazas e implantación de controles de seguridad que mitiguen estas, con el fin de garantizar la confidencialidad, la autenticidad y la integridad de la información.

RED.ES

Red.es es la entidad pública empresarial adscrita al Ministerio de Industria, Turismo y Comercio (MITyC) encargada de impulsar el desarrollo de la Sociedad de la Información en España y ejecutar proyectos de acuerdo a las prioridades estratégicas de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) interactuando con Comunidades Autónomas, Diputaciones, entidades locales y el sector privado en materia de tecnologías de la información y comunicaciones (TIC).

Entre sus funciones se incluyen las siguientes:

- Gestionar el registro de nombres de dominio de Internet bajo el código de país.es

- Impulsar el despliegue del DNI electrónico mediante la instalación del equipamiento necesario y la gestión del servicio de cita previa.

- Llevar a cabo iniciativas para sensibilizar a diferentes colectivos y a la ciudadanía en general en el uso de las Tecnologías de la Información y la Comunicación como el archivo de la experiencia o el programa Chaval.es.

- Promover la incorporación de las nuevas tecnologías en las PyMES a través del impulso de la empresa en red, con programas específicos como NEW o jornadas empresas en red de sensibilización en el uso de las TIC a empresarios.

Entre los órganos adscritos a Red.es, destaca ONTSI (Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información), cuyo objetivo es el estudio y análisis de la Sociedad de la Información en España, y RedIRIS.

RedIRIS es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Está financiada por el Ministerio de Ciencia e Innovación, e incluida en su mapa de Instalaciones Científico Tecnológicas Singulares. Se hace cargo de su gestión la entidad pública empresarial Red.es, del Ministerio de Industria, Turismo y Comercio. RedIRIS cuenta con más de 340 instituciones afiliadas, principalmente universidades y centros públicos de investigación. RedIRIS ofrece a la comunidad académica y científica española servicios de comunicaciones, con una infraestructura de transporte adaptada tecnológicamente a las necesidades de los centros e instituciones usuarias. RedIRIS ofrece asimismo servicios de *middleware*, entendidos como una capa entre la red y las aplicaciones, encargada de facilitar tareas como identificación, autenticación, autorización, gestión de la seguridad y movilidad. El uso de esta capa permite a las aplicaciones sacar un mayor provecho de la red e interoperar por medio de interfaces normalizadas, ofreciendo así a los usuarios servicios más avanzados con un menor esfuerzo.

Dentro del área de Seguridad en Red, RedIRIS ha sido pionera en la implantación y operación de diversos servicios de seguridad para las redes académicas y de investigación españolas, como son:

- Eduroam - Acceso federado a la red para usuarios móviles

- IRIS-CERT - Servicio de seguridad de RedIRIS

- IRISRBL - Listas IP de reputación
- Keyserver - Servidor de claves PGP
- pkIRISGrid - PKI para la e-Ciencia española
- SCS - Servicio de certificados de servidor para la comunidad RedIRIS
- SIR - Servicio de identidad de RedIRIS
- RID - Registro de identidad digital

Capítulo 7

Catálogo de grupos de I+D en la universidad

7. Catálogo de grupos de I+D en la universidad

Existen múltiples grupos de investigación en las universidades y centros de investigación españoles que tienen toda o parte de su actividad investigadora alrededor de los temas de seguridad en red. A continuación, se exponen un conjunto de los más relevantes dentro del área de seguridad en redes de telecomunicación.

Grupo NQAS. EHU

- Universidad del País Vasco. Departamento de Electrónica y Telecomunicaciones.

- Web: http://det.bi.ehu.es/NQAS/

- Email: alex.munoz@ehu.es

- Dirección: Escuela Técnica Superior de Ingeniería de Bilbao. Alameda de Urquijo s/n. 48013 Bilbao.

- Seguridad en redes de datos.

Grupo I2T. EHU

- Universidad del País Vasco. Departamento de Electrónica y Telecomunicaciones.

- Web: https://www.i2t.ehu.es/

- Email: i2t@ehu.es

- Dirección: Escuela Técnica Superior de Ingeniería de Bilbao. Alameda de Urquijo s/n. 48013 Bilbao.

- Seguridad en sistemas distribuidos. Seguridad a nivel de enlace en redes inalámbricas y cableadas. Soluciones AAA basadas en PKI. Análisis de seguridad.

Grupo de criptología y seguridad computacional. UA

- Universidad de Alicante. Departamento de Ciencia de la Computación e Inteligencia Artificial.

- Web: http://www.dccia.ua.es/csc/

- Email: zamora@dccia.ua.es

- Dirección: Campus de Sant Vicent. Ap. Correus, 99. E-03080 Alacant.

- Técnicas criptográficas aplicaciones a la seguridad de la información. Criptoanálisis de sistemas.

Grupo de redes y middleware. UA

- Universidad de Alicante. Departamento de Tecnología Informática y Computación, adscrito al Instituto Universitario de Investigación Informática.

- http://www.dtic.ua.es/grupoM/inicio.jsp?lang=es

- Email: info.grupom@dtic.ua.es

- Dirección: Carretera San Vicente s/n. 03690 San Vicente (Alicante).

- Modelos de seguridad de red basados en tecnologías de computación distribuida.

Grupo del departamento de ingeniería de la información y de las comunicaciones (dEIC). UAB

- Universidad Autónoma de Barcelona - Departament d'Enginyeria de la Informació i de les Comunicacions.

- Web: http://ccd.uab.es

- Email: webadmin@deic.uab.cat

- Dirección: Edifici Q. Universitat Autònoma de Barcelona. 08193 - Bellaterra - Cerdanyola del Vallès (Barcelona).

- Criptografía y seguridad computacional, estudio de protocolos para la compartición de secretos y en sus aplicaciones a la transferencia segura de información a través de les redes telemáticas.

Grupo de ingeniería de servicios telemáticos. UAH

- Universidad Alcalá de Henares. Departamento de Automática.

- Web: http://www.it.aut.uah.es/ist/

- Email: secre@aut.uah.es

- Dirección: Departamento de Automática - Edificio Politécnico (Zona Este), Campus N-II, 28871 Alcalá de Henares (Madrid).

- Seguridad en el entorno de agentes. Esta línea aborda tanto las arquitecturas de seguridad e identificación, como la prevención y actuación ante posibles ataques a los sistemas.

Grupo de redes. UAM

- Universidad Autónoma de Madrid.

- Web: http://nrg.ii.uam.es/

- Email: jorge.lopez_vergara@uam.es

- Dirección: Escuela Politécnica Superior. Universidad Autónoma de Madrid (UAM). Francisco Tomás y Valiente, 11. 28049 Madrid.

- Diseño y formalización de políticas de seguridad en red.

Grupo del departamento de electrónica y sistemas. UAX

- Universidad Alfonso X el Sabio - Escuela Politécnica Superior.

- Web: http://www.uax.es/

- Email: jortega@uax.es

- Dirección: Avenida Universidad, 1. 28691 Villanueva de la Cañada (Madrid).

- Estudio de protocolos y sistemas de seguridad aplicados a redes inalámbricas. Especial dedicación a todos los sistemas aplicables a redes WLAN, y más en concreto para los protocolos de la familia IEEE 802.11.

Grupo de seguridad de las tecnologías de la información y de las comunicaciones. UC3M

- Universidad Carlos III de Madrid. Escuela Politécnica Superior.

- Web: http://www.seg.inf.uc3m.es/

- Email: arturo@inf.uc3m.es

- Dirección: Avenida de la Universidad, 30. 28911 Leganés (Madrid).

- Investigación en seguridad aplicada a los servicios de localización y los basados en la localización, aplicación de la firma electrónica y los servicios de certificación, estándares de seguridad en XML y tecnologías RFID.

Grupo Alarcos. UCLM

- Universidad Castilla La Mancha. Escuela Superior de Informática de Ciudad.

- Web: http://alarcos.inf-cr.uclm.es

- Email: alarcos@inf-cr.uclm.es

- Dirección: Escuela Superior de Informática de Ciudad Real Paseo de la Universidad, 4. 13071 Ciudad Real.

- Proceso para el desarrollo de sistemas seguros basados en servicios web, con especial énfasis en aspectos relacionados con requisitos, arquitectura y patrones de seguridad.

Grupo de análisis, seguridad y sistemas (GASS). UCM

- Universidad Complutense de Madrid. Departamento de Ingeniería del Software e Inteligencia Artificial.

- Web: http://gass.ucm.es/

- E-mail: gass@fdi.ucm.es

- Dirección: Facultad de Informática. Universidad Complutense de Madrid (UCM) Despacho 431. c/ Profesor José García Santesmases, s/n. Ciudad Universitaria. 28040 Madrid.

- Diseño, evaluación e implementación de algoritmos criptográficos y protocolos. Desarrollo de arquitecturas de seguridad para sistemas de información y de comunicaciones.

Grupo de investigación en señales, telemática y comunicaciones. UGR

- Universidad de Granada. Departamento de Teoría de la Señal, Telemática y Comunicaciones.

- Web: http://tstc.ugr.es/

- Email: jedv@ugr.es

- Dirección: ETS Ing. Informáticas y de Telecomunicación - c/ Periodista Daniel Saucedo Aranda, s/n. 18071 Granada.

- Seguridad en redes. Sistemas de detección y respuesta ante intrusiones.

Grupo del departament de ciències matemàtiques i informàtica. UIB

- Universidad de les Illes Balears. Departament de Ciències Matemàtiques i Informàtica.

- Web: http://dmi.uib.es/spip.php?article47

- Email: hola@dmi.es

- Dirección: Universitat de les Illes Balears. Cra. de Valldemossa, km 7.5. Palma (Illes Balears).

- Seguridad en redes telemáticas. Comercio electrónico. Administración electrónica.

Grupo de criptología (CryptULL). ULL

- Universidad de La Laguna. Departamento de Estadística, Investigación Operativa y Computación.

- Web: http://webpages.ull.es/users/cryptull/

- Email: pcaballe@ull.es

- Dirección: Campus de Anchieta. 4ª Pta. Edif. Física y Matemáticas. c/ Astrofísico F. Sánchez, s/n. 38271 La Laguna.

- Seguridad en redes inalámbricas.

Grupo ANTS. UM

- Universidad de Murcia. Departamento de Ingeniería de la Información y las Comunicaciones.

- Web: http://ants.dif.um.es/

- Email: ants-admin@dif.um.es

- Dirección: Avda. Teniente Flomesta, 5. 30003 Murcia.

- Servicios de seguridad avanzados y AAA sobre redes IP.

Grupo de ingeniería del software (GISUM). UMA

- Universidad de Málaga. ETS. Ing. Informática.

- Web: http://www.lcc.uma.es/~gisum/

- Email: jlm@lcc.uma.es

- Dirección: Campus de Teatinos. 29071 Málaga.

- Seguridad en sistemas y aplicaciones distribuidas.

Grupo de telemática. Universidad de Mondragón

- Universidad de Mondragón.

- Web: http://www.mondragon.edu/telematika/

- Email: t2@eps.mondragon.edu

- Dirección: Loramendi, 4. 20500 Mondragón (Guipúzcoa).

- Sistemas de detección de intrusiones (IDS). Sistemas trampa (honeypots & honeynets). Seguridad en sistemas empotrados. Sistemas anti-spam.

Grupo de tecnología de las comunicaciones. UNIZAR

- Universidad de Zaragoza. Departamento de Ingeniería Electrónica y Comunicaciones.

- Web: http://diec.unizar.es/~gtc/

- Email: sed5008@unizar.es

- Dirección: Centro Politécnico Superior. c/ María de Luna, 1. 50018 Zaragoza.

- Seguridad, optimización y diseño de redes de comunicaciones.

Grupo KISON. UOC

- Universitat Oberta de Catalunya.

- Web:http://www.uoc.edu/opencms/opencms/webs/grups_de_recerca/Kison/EN/

- Email: dmegias@uoc.edu

- Seguridad en redes ad-hoc.

Grupo de seguridad en red. UPC

- Universidad Politècnica de Catalunya. Departament d'Arquitectura de Computadors.
- Web: http://research.ac.upc.edu/cnds/
- Email: medina@ac.upc.es
- Dirección: c/ Jordi Girona, 1-3, D6 Campus Nord. 08034 Barcelona.
- Seguridad en red.

Grupo de integración de redes y servicios: UPC

- Escuela Universitaria Politécnica de Mataró.
- Web: http://www.eupmt.es/document.php?id=135
- Email: escola@eupmt.es
- Dirección: avda. Puig i Cadafalch, 101-111. 08303 Mataró
- Seguridad (protección y detección, auditorías).

Grupo de sistemas telemáticos para la sociedad de la información y el conocimiento. UPM

- Universidad Politécnica de Madrid. Departamento DIATEL.
- Web: http://www.diatel.upm.es/investigacion/Seguridad.html
- Email: agomez@diatel.upm.es
- Dirección: Crta. Madrid-Valencia, km 7. 28031 Madrid.
- Definición de políticas de seguridad para entornos de trabajo en red y aplicar mecanismos de seguridad a aplicaciones de comunicaciones.

Grupo de laboratorio de criptología. UPM

- Universidad Politécnica de Madrid. Facultad de Informática.
- Web: http://tirnanog.ls.fi.upm.es/
- Email: adminweb@dilmun.ls.fi.upm.es
- Dirección: Facultad de Informática. Campus de Montegancedo, s/n. 28660 Boadilla del Monte (Madrid).
- Aplicación de la criptografía a las comunicaciones.

Grupo de redes y servicios de telecomunicación e internet. UPM

- Universidad Politécnica de Madrid. Dpto. de Ingeniería Telemática.
- Web: http://www.dit.upm.es/rsti
- Email: gi.rsti@upm.es
- Dirección: ETSI de Telecomunicación. Ciudad Universitaria, s/n. 28040 Madrid.
- Uso de lenguajes formales para políticas de seguridad. Sistemas de Respuesta a Intrusiones. Aplicación de Virtualización para despliegue dinámico de señuelos.

Grupo del laboratorio de sistemas integrados. UPM

- Universidad Politécnica de Madrid. Departamento de Ingeniería Electrónica.
- Web: http://www.lsi.die.upm.es/
- Email: webmaster@die.upm.es
- Dirección: ETSI de Telecomunicación. Ciudad Universitaria, s/n. 28040 Madrid.
- Seguridad en Sistemas Empotrados.

Grupo de investigación en tecnología informática y de las comunicaciones. UPM

- Universidad Politécnica de Madrid. Facultad de Informática.
- Web: http://www.cettico.fi.upm.es
- Email: gi.cetico@upm.es
- Dirección: Facultad de Informática. Campus de Montegancedo, s/n. 28660 Boadilla del Monte (Madrid).
- Seguridad en Internet.

Grupo de redes de computadores. UPV

- Universidad Politécnica de Valencia. Departament d'Informàtica de Sistemes i Computadors.
- Web: http://www.grc.upv.es/
- Email: webadmin@grc.upv.es
- Dirección: Camí de Vera, s/n. 46022 Valencia.
- Autorización de dispositivos y usuarios basada en el intercambio de claves y gestión de las mismas en entornos sin infraestructura centralizada, disponibilidad de la red y encaminamiento seguro.

Grupo CRISES. URV

- Universitat Rovira i Virgili. Departamento de Informática y Matemáticas.
- Web: http://crises-deim.urv.cat/webCrises/index.php
- Email: josep.domingo@urv.cat
- Dirección: avda. Països Catalans, 26. E-43007 Tarragona.
- E-commerce seguro.

Grupo QUIVIR. US

- Universidad de Sevilla. Dpto. de Lenguajes y Sistemas Informáticos.

- Web: http://www.lsi.us.es/~quivir/

- Email: quivir@lsi.us.es

- Dirección: ETS de Ingeniería Informática. Avda. Reina Mercedes, s/n. 41012 Sevilla.

- Políticas de seguridad y cortafuegos. IDS. Respuesta a intrusiones. Lenguajes de políticas de seguridad.

Capítulo 8

La seguridad en redes en el 7º programa marco de investigación de la UE

8. La seguridad en redes en el 7º programa marco de investigación de la UE

Los Programas marcos (*Framework Programmes*-FP) son los principales instrumentos de financiación usados por la Unión Europea para promover las actividades de Investigación y Desarrollo en casi todas las disciplinas científicas.

El programa marco actualmente en vigor es el Séptimo Programa marco, (FP7), que incluye una planificación para 7 años, desde 2007 a 2013, y con un presupuesto de 50.521 millones de Euros.

La estructura del programa marco son cuatro programas:

- Cooperación: se incluyen las actividades de investigación de cooperación transnacional.

- Ideas: para promover la investigación en aspectos muy avanzados.

- Personas: para promover la generación y movilidad de investigadores.

- Capacidades: para promover la creación y mantenimiento de infraestructuras de investigación.

El programa más importante en cuanto a actividad y presupuesto es el de cooperación, en el cual se financian los proyectos colaborativos, que constituyen el núcleo de la financiación de la investigación de la UE.

Estos proyectos colaborativos están estructurados en 10 grandes temas, entre los que se encuentra un tema dedicado a seguridad, pero más orientado a la seguridad de infraestructuras, y otro tema dedicado a tecnologías de la información y comunicaciones, donde se encuadra claramente los aspectos de seguridad en red. Este tema está estructurado en siete "retos" (*challenges*), que incluyen aspectos relacionados con la seguridad en las redes de comunicación. Las iniciativas más importantes de financiación para la investigación en seguridad en redes se concentran en el ICT Challenge 1: "*Pervasive and Trusted Network and Service Infrastructures*", dentro del área "*Secure, dependable and trusted infrastructures*" (Objetivo 1.4).

Esta área persigue los siguientes objetivos:

- Seguridad y sostenibilidad de infraestructuras de red. Se buscan iniciativas para construir y desarrollar arquitecturas y tecnologías flexibles, escalables, seguras y sensibles al contexto que permitan una transmisión segura de datos y servicios a través de redes e infraestructuras heterogéneas, incluyendo redes dinámicas de sensores, detección y recuperación de intrusiones en tiempo real, etc.

- Seguridad y confianza en arquitecturas de servicio dinámica y reconfigurables, que permitan ofrecer combinaciones y coaliciones de servicios de una forma segura y escalable.

- Infraestructuras confiables de computación, que permitan una interoperabilidad y seguridad extremo a extremo de los datos y los servicios.

- Gestión de identidad y herramientas para mejorar la privacidad.

Los proyectos más significativos (IPs: *Integrated Projects*) que están actualmente en curso son [29]:

- MASTER (*Managing Assurance, Security and Trust for Services*): su objetivo es proporcionar metodologías e infraestructuras para facilitar la monitorización, ejecución y auditoría de indicadores cuantificables de la seguridad de un proceso de negocio. Se proporcionará una garantía de seguridad gestionable y niveles de confianza de arquitecturas dinámicas orientadas a servicio en tres escenarios: centralizado, distribuido y externalizado.

- PRIMELIFE (*Privacy and Identity Management in Europe for Life*): su objetivo es contribuir a proteger la privacidad en nuevas aplicaciones de Internet, tales como escenarios colaborativos y comunidades virtuales.

- TAS3 (*Trusted Architecture for Securely Shared Services*): su objetivo es desarrollar e implementar una arquitectura con servicios confiables para gestionar y procesar información personal distribuida.

- TECOM (*Trusted Embedded Computing*): su objetivo es el desarrollo de sistemas empotrados de confianza, con plataformas hardware que integran componentes confiables.

- TURBINE (*Trusted Revocable Biometric Identities*): propone una novedosa tecnología de autenticación basada en desarrollos criptográficos y de biometría de huella de dedo, aplicada a la gestión de identidad.

Otros proyectos con menor volumen (*STREPS: Specific Trageted Research projects*), son:

- ACTIBIO: *Unobtrusive Authentication Using Activity Related and Soft Biometrics*.

- AVANTSSAR: *Automated Validation of Trust and Security of Service oriented Architectures*.

- AWISSENET: *Ad-hoc PAN and WIreless Sensor SEcure NETwork*.

- CACE: *Computer Aided Cryptography Engineering*.

- Consequence: *Context-aware data-centric information sharing*.

- GEMOM: *Genetic Message Oriented Secure Middleware*.

- INTERSECTION: *INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks*.

- MOBIO: *Mobile Biometry*.

- PICOS: *Privacy and Identity Management for Community Services*.

- PRISM: *Privacy-aware Secure Monitoring*.

- SecureSCM: *Secure Supply Chain Management*.

- SHIELDS: *Detecting known security vulnerabilities from within design and development tools*.

- SWIFT: *Secure Widespread Identities for Federated Telecommunications*.

- WOMBAT: *Worldwide Observatory of Malicious Behaviours and Attack Threats*.

Referencias

1. Spafford, E. "*An analysis of the Internet Worm*." *Proceedings of the European Software Engineering Conference*. 1989.

2. Reynolds, J. "*The Helminthiasis of the Internet*." Request For Comments 1135 , 1989.

3. Mañas, J. A. *Mundo* IP. Madrid: Nowtilus, 2004.

4. UNE-ISO/IEC-17799. "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información." 2002.

5. Ministerio de Administraciones Públicas. "MAGERIT - versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información." Madrid, 2006.

6. Pfleeger, S., y S. Pfleeger. *Security in Computing*. New Jersey: Pearson, 2003.

7. Scambray, J., S. McClure, y G. Kurtz. *Hacking Exposed: Network Security Secrets & Solutions*. meryville, CA: McGraw-Hill, 2005.

8. Bellovin, S. "*Security Problems in the TCP/IP Protocol Suite*." *Computer Communication Review* 19 (April 1989): 32-48.

9. "*IP-Spoofing Demystified, Trust-Relationship Exploitation*." *Phrack Magazin*e 7, nº 48 (June 1996): 1-9.

10. Alvarez-Marañón, G. *Seguridad Informática para empresas y particulares*. Madrid: McGraw-Hill, 2004.

11. Aycock, J. *Computer Viruses and Malware (Advances in Information Security)*. Springer, 2006.

12. Carracedo, J. *Seguridad en Redes Telemáticas*. Madrid: McGraw Hill, 2004.

13. Stallings, W. *Criptography and Network Security*. Prentice Hall, 2006.

14. Kuhn, M., y R. Anderson. *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*. Vol. 1525/1998, de *Information Hiding*, 124-142. Springer Berlin / Heidelberg, 1998.

15. Ortega, J., y F. Alonso. *Biometría y Seguridad*. Madrid: Cuadernos Cátedra ISDEFE-UPM, 2008.

16. Massachussets Institute of Technology. "*Teaching Students About Responsible Use of Computers*." *Communications of the ACM* 32, nº 6 (June 1989): 704.

17. Tung, B. Kerberos: a *Network Authentication System*. Addison-Wesley, 1999.

18. Rosenberg, J., y D. Remy. *Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature and XML Encryption*. Sams, 2004.

19. Nakhjiri, M., y M. Nakhjiri. *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*. Wiley, 2005.

20. Cheswick, W., S. Bellovin, y A. Rubin. *Firewalls and Internet Security. Repelling the Wily Hacker*. Addison-Wesley, 2003.

21. Malik, S. *Network Security Principles and Practices*. Cisco Press, 2002.

22. Chapman, D. B., y S. Coopers. *Building Internet Firewalls*. Cambridge, MA: O'Reilly Associates, 2000.

23. Chapman, B. "*Network (In) Security through IP Packet Filtering*." USENIX: *Proceedings of the Third UNIX Security Symposium*. Baltimore, MD, 1992.

24. Yuan, R., y W. Strayer. *Virtual Private Networks: Technologies and Solutions*. Addison-Wesley, 2001.

25. Amoroso, E. *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response*. Intrusion.Net, 1999.

26. Stakhanova, N., S. Baso, y J. Wong. "*A taxonomy of Intrusion Response Systems*." *Internation Journal of Information and Computer Security 1*, nº 112 (2007).

27. Honeynet Project. *Know Your Enemy: Learning about Security Threats*. Addison-Wesley, 2004.

28. INTECO. "Estudio sobre el sector de la seguridad TIC en España." 2008.

29. European Commission. Information Society and Media. "*Synopsis of R&D Projects. Work Programme 2007-2008. Challenge 1, Objective 1.4: "Secure, dependable and trusted Infrastructures*"." 2008.

Índice de figuras Pág.

En este cuaderno se hace una revisión de las principales tecnologías existentes para proteger la infraestructura de sistemas de información de una organización de los potenciales ataques que se dan actualmente. Por ello, se describen, en primer lugar, los tipos y mecanismos de ataques que pueden introducirse a través de la conexión de una organización a redes abiertas como es Internet. Una vez descritos los ataques, se profundiza en el estudio de las distintas tecnologías de control de acceso existentes para protegerse de dichos ataques, desde la necesaria mención al control de acceso físico, a las distintas técnicas de control de acceso lógico: sistemas de autenticación y sistemas de defensa perimetral. En el cuaderno, se proporciona una visión global de las tecnologías de control de acceso a través de su categorización y la descripción de su funcionalidad, así como el detalle técnico de aquellas más relevantes actualmente.

Víctor A. Villagrá González
Profesor Titular de Universidad
Grupo de Redes y Servicios de Telecomunicación e Internet
Departamento de Ingeniería de Sistemas Telemáticos
E.T.S.I. de Telecomunicación-UPM