1 Seguridad en la Web, Problemática, Sistemas y Políticas de Seguridad

1.1 Introducción

Hoy en día, el éxito de una empresa depende en gran medida de la calidad de la información que genera y gestiona. La información comprende los datos propios que gestiona, los mensajes que se intercambian entre las personas y/o las máquinas de la organización, el historial de clientes y proveedores, de productos, etc. En definitiva, la información representa el *know-how* de la organización y si ésta se pierde o deteriora, le será muy difícil recuperarse y seguir siendo competitiva. Se dice que una empresa posee información de calidad si, además de ser útil en su operativa, presenta otras características adicionales como son la confidencialidad, la integridad y la disponibilidad. Es en este momento, cuando se trata de dotar de seguridad a los sistemas de información que la empresa utiliza. Así pues, puede decirse que la seguridad es el conjunto de medidas que las organizaciones adoptan con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. Cuando el acceso a la información de la organización se realiza a través de servicios telemáticos (como ocurren en el caso de Internet) la necesidad de adoptar estas medidas es insoslayable. En concreto, son cuatro los elementos fundamentales de la seguridad informática cuyas definiciones se han extraído de CSI (1996):

- *Confidencialidad*, que puede definirse como la característica que previene contra la divulgación no autorizada de la información.

- *Autenticación*, definida como la propiedad de dar y reconocer la autenticidad de la información y/o la identidad de los actores (típicamente una fuente y un destinatario de los datos) y/o la autorización por parte de los autorizadores, así como, la verificación de dichas tres cuestiones.

- *Integridad*, definida como la característica que previene contra la modificación o destrucción no autorizadas de la información de una organización.

- *Disponibilidad*, o característica que previene contra la denegación no autorizada de acceso a la información.

La necesidad de adoptar medidas de seguridad que protejan la información de una empresa se debe a que en el entorno en que ésta se desenvuelve (personas, máquinas, sucesos o ideas) existen amenazas, es decir, condiciones de dicho entorno que, dada una oportunidad, podrían dar lugar a que se produjese una violación de la seguridad. Ejemplos de amenazas de seguridad son: la divulgación no autorizada de la información, la modificación no autorizada de la información, el acceso no autorizado a recursos, la denegación de un servicio. Para hacer frente a estas amenazas y, por lo tanto, para protegerse o paliar los efectos de la materialización de una de estas amenazas, se dispone de servicios de seguridad, los cuales establecen qué hacer frente a estas amenazas con el fin de satisfacer los requisitos de seguridad de la organización. Ejemplos de servicios de seguridad son: la confidencialidad de los datos, la integridad de los datos y el control de acceso. Una vez identificadas las medidas a adoptar ante las posibles amenazas, es necesario implementar dichas medidas, para lo cual se acudirá a las técnicas y mecanismos de seguridad concretos que soportan la lógica y los algoritmos que implementan los servicios considerados. Ejemplos de técnicas y mecanismos de seguridad son: la criptografía, los cortafuegos (*firewalls*), las firmas digitales, etc. Por último, es importante resaltar que la identificación de las amenazas y la definición e implementación de las oportunas medidas, debe hacerse en el marco de un plan de seguridad de la empresa que defina una política de seguridad, es decir, un documento que defina los objetivos de seguridad en función de las necesidades propias de la organización y asigne responsabilidades en la gestión de la seguridad.

1.2 Amenazas de seguridad

El estudio de la seguridad informática puede plantearse desde dos enfoque diferentes:

- *Seguridad física*, o protección del sistema ante amenazas físicas (desastres naturales, incendios, agua, robo y pirateo informático, etc.) y requiere la definición de planes de contingencia, así como, el establecimiento de una política de control de acceso físico al sistema, de una política de copias de seguridad, etc.

- *Seguridad lógica*, o protección de la información en su propio medio, es decir, en las aplicaciones informáticas que soportan tal información. Por lo general, se emplearán técnicas criptográficas para lograr este fin.

En cualquier caso deben asumirse los siguientes principios de cara a garantizar la seguridad.

- En primer lugar hay que ser conscientes de que el atacante utilizará cualquier artilugio que haga más fácil su acceso y su posterior ataque. Esto conduce a identificar los puntos débiles de cualquier sistema informático, y evaluar mediante un análisis de riesgos, no sólo la posibilidad de la amenaza, sino el perjuicio ocasionado en caso de materializarse.

- También hay que tener presente que sólo debe protegerse la información mientras ésta tenga valor, por lo que tiene sentido hablar de la caducidad de los sistemas de protección.

- Por último, las medidas de seguridad deberán estar implementadas de forma que su funcionamiento sea eficaz (que proporcionen la respuesta apropiada en el momento oportuno), eficiente (que optimicen los recursos del sistema) y fáciles de usar (que pasen desapercibidas para el usuario).

Por lo tanto, una de las primeras cuestiones a la hora de abordar el problema de la seguridad es identificar las debilidades del sistema. Estas pueden referirse básicamente a cinco entidades distintas: el hardware (conexiones sueltas, desconexión de tarjetas, etc.), el software (robo de programas, modificación, ejecuciones incorrectas, etc.), los datos (alteración de contenidos, introducción de datos falsos, manipulación fraudulenta, etc.), la memoria (virus, mala gestión de memoria, bloqueo del sistema, etc.) y los usuarios (suplantación de la identidad, accesos no autorizados, etc.). De estos cinco elementos, los tres primeros son los que sufren un mayor número de ataques y constituyen lo que se denomina el *triángulo de las debilidades del sistema* (véase la Figura 1).

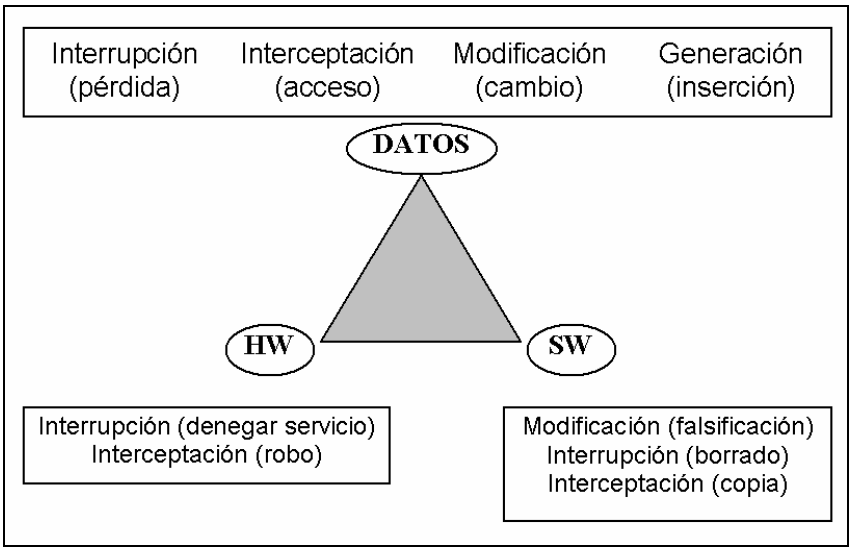

Figura 1: El triángulo de las debilidades de los sistemas informáticos.

Así pues, interesa conocer cuales son las amenazas que afectan a los tres elementos claves (hardware, software y datos), entendiendo genéricamente por amenaza cualquier condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad,

podría dar lugar a que se produjese una violación de la seguridad. Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente *A* (como por ejemplo un fichero o una región de la memoria principal) a un destino *B* (como por ejemplo otro fichero o un usuario). Las cuatro categorías generales de amenazas son las siguientes y se ilustran en la Figura 2.

- *Interrupción*, un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación, eliminar un programa o un conjunto de datos, etc.

- *Interceptación*, una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- *Modificación*, una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transmitidos a través de la red.

- *Generación*, una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

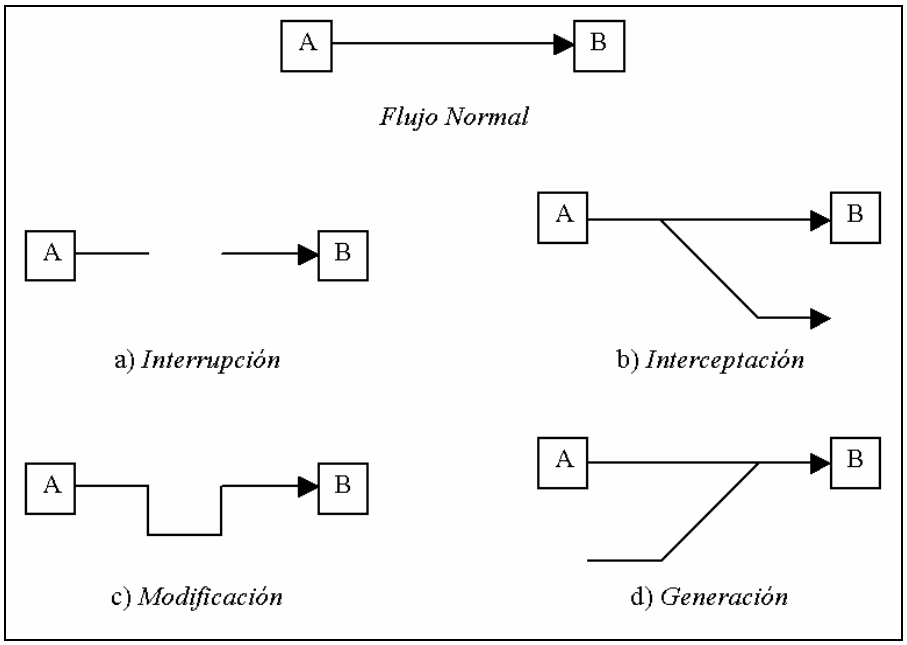

Figura 2: Clasificación de las amenazas según la modificación realizada sobre el flujo normal de datos entre una fuente y un destino.

A la vista de la Figura 1 se comprende que los datos son la parte del sistema más vulnerable, por lo que en este curso se centrará la atención en el estudio de los mecanismos disponibles para garantizar la seguridad de los datos.

Por abuso del lenguaje, muchas veces se emplea el término ataque como sinónimo de amenaza, si bien, un ataque es realmente la materialización de una amenaza. Genéricamente, se diferencian dos tipos de ataques:

- *Ataques pasivos*. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza con el fin de obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Este último ataque constituye una técnica más sutil para obtener información relativa a la obtención del origen y destinatario de la comunicación (mediante la lectura de las cabeceras de los paquetes monitorizados), el control del volumen de tráfico intercambiado entre las entidades monitorizadas (obteniendo así información acerca de los períodos de actividad e inactividad normales o inusuales). Los ataques pasivos son difíciles de detectar, ya que no provocan ninguna alteración de los datos, y pueden realizarse mediante aplicaciones conocidas como *sniffers*.

- *Ataques activos*. Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos y son los que habitualmente suelen sufrir los sistemas informáticos.

1.3 Servicios de seguridad

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Los servicios de seguridad suelen agruparse en función de la propiedad de la información que tratan de salvaguardar.

- *Confidencialidad*. El servicio de confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o, tal vez, sólo a porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. El servicio de confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo, produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

- *Autenticación*. Este tipo de servicios son imprescindibles cuando se requiere una identificación correcta del origen o destino del mensaje, asegurando que no se trata de falsas entidades. Se distinguen dos tipos: autenticación de entidad (o comprobación de que una entidad es la que se presupone) y de datos de origen (o comprobación de que la fuente de los datos recibidos es la afirmada). Este servicio trata de combatir fundamentalmente la amenaza del enmascaramiento.

- *Integridad*. En este caso, se requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reenvío de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo anexando al mensaje original un resumen cifrado del mismo (o firma digital), mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo, mediante *timestamps*.

- *No repudio y Acuse de recibo*. El servicio de no repudio proporciona al emisor/receptor de un mensaje, una prueba irrefutable de que el contenido recibido fue el mismo que el del mensaje enviado por el emisor y que, por lo tanto, no ha habido modificación del mismo desde el emisor, y se aceptará el mensaje. La presencia de un certificado de no repudio, prueba que el receptor aceptó la notificación de no repudio solicitado por el emisor. Este servicio protege al emisor/receptor de un documento, de cualquier intento por parte del origen/destino de negar su envío/recepción en su totalidad o en parte del contenido del mismo. Asimismo, pretende dar una validez legal a un documento, ya que requiere que una persona se responsabilice del contenido del documento estampando su firma digital en él. Ahora bien, otro problema diferente es el de poder demostrar que un mensaje ha llegado a su destino. En este caso, la posición del emisor puede quedar comprometida ya que el receptor puede alegar que no

recibió mensaje alguno o lo que es lo mismo, negar su existencia. Para que el emisor esté seguro de que el mensaje ha llegado a su destino, aparece la figura del acuse de recibo (o mensaje del receptor al emisor confirmando la recepción del mismo). Ahora bien, es en este punto cuando se invierten las posiciones, pues el receptor no puede justificar que envió el acuse de recibo, estaríamos dentro de un círculo vicioso de envíos y contra envíos de acuses de recibo. Para solucionar este problema, se impone la figura de una tercera parte de confianza o fiable (*TTP, Trusted Third Party*), siendo a través de su actuación la forma de que se logre que todas las partes tengan prueba plena del origen, contenido y destino de cualquier mensaje que se haya emitido o recibido.

- *Control de acceso*. También se requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas, llaves hardware, cortafuegos, etc.

1.4 Mecanismos de seguridad

Los servicios de seguridad definen qué medidas son necesarias adoptar para garantizar los requisitos de seguridad de un sistema, mientras que las técnicas y mecanismos de seguridad determinan cómo se implementan tales medidas. Así pues, una técnica o mecanismo de seguridad es la lógica o algoritmo que implementa un servicio de seguridad particular, bien sea en hardware o software. Aunque no existe un único mecanismo capaz de proveer todos los servicios de seguridad, la mayoría de ellos hacen uso de técnicas criptográficas (Lucena, 2002; Schneier, 1996) basadas en el cifrado de la información.

A continuación se ofrece un recorrido por el "bazar" de las técnicas y mecanismos disponibles para lograr cada uno de los servicios de seguridad comentados en el apartado anterior. Así, para el caso de los servicios orientados a garantizar la confidencialidad de los datos o del flujo de datos se emplean técnicas y métodos como:

- *Cifrado*. Garantiza que la información es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar mediante un proceso de cifrado un texto plano en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para implementar otras mecanismos como la autenticación, la distribución de claves y las firmas digitales.

- *Etiquetas de seguridad*. Los recursos, incluyendo los datos, pueden tener asociadas etiquetas de seguridad, por ejemplo, para indicar el nivel de sensibilidad (a la difusión).

- *Relleno de tráfico*. Los mecanismos de relleno del tráfico se pueden utilizar para proporcionar diversos niveles de protección contra los análisis del tráfico. Se trata de enviar tráfico espurio junto con los datos válidos para que el "adversario" no sepa si se está enviando información o qué cantidad de datos útiles se está transfiriendo. Estos mecanismos sólo pueden ser efectivos si el relleno del tráfico está protegido mediante un método de cifrado.

Para implementar otros servicios, los mecanismos o técnicas empleadas son muy variadas:

- Códigos MAC (*Message Authentication Codes*). Este tipo de códigos se emplean para garantizar la integridad de un mensaje de datos. Los códigos MAC son también etiquetas de autenticación que se obtienen de la aplicación de un mecanismo de autenticación (básicamente, funciones resumen[1] o algoritmos de cifrado de clave secreta), junto con una

[1] Las funciones resumen (*hash functions*) son funciones sin inversa, por lo que si se aplican sobre un mensaje de datos a transmitir, es imposible reconstruir el mensaje original a partir del resumen generado y, además, por su diseño es muy improbable que dos mensajes diferentes generen el mismo resumen. Estas funciones pueden emplearse para implementar un servicio que garantice la integridad (códigos MAC) o la autenticación de un origen de datos (firmas digitales).

clave secreta, a partir de los datos a transmitir. Los códigos MAC se caracterizan porque los procesos de generación y verificación utilizan la misma clave.

- *Firmas digitales*. La autenticación del origen de datos puede garantizarse mediante este mecanismo. Se basa en el uso de técnicas criptográficas y suele implementarse con técnicas de cifrado de clave pública. La posesión de una clave privada identifica a un usuario ya que ésta sólo es conocida por el propietario, y, sólo él puede cifrar con ella. Todo el mundo puede verificar la identidad de un usuario descifrando con la clave pública los datos cifrados con la privada. Si son iguales, la firma es correcta, en caso contrario se rechaza. La característica esencial del mecanismo de firma, es que dicha firma sólo puede haber sido generada con la información privada del signatario. Por lo tanto cuando se verifica la firma, se puede probar que sólo el poseedor de la información privada puede haberla generado.

- *Terceras partes de confianza* (*TTP*, *Trusted Third Parties*). Para implementar un servicio de no repudio o un servicio de acuse de recibo, es necesario, además de la utilización de firmas digitales, la participación de una tercera parte en la que ambos interlocutores (origen y destino) confían y cuya misión es arbitrar en situaciones de conflicto (existencia o no de un mensaje, negación de la existencia de un mensaje por una de las partes, etc.), de forma que, a requerimiento de uno o ambos interlocutores, la TTP emite un informe de resolución de tales conflictos.

- *Intercambio de autenticaciones*. La autenticación de entidades puede realizarse mediante técnicas de intercambio basadas en la utilización de una información de autenticación (como contraseñas proporcionadas por la entidad emisora y comprobadas por la entidad receptora) o técnicas criptográficas. Si el mecanismo no proporciona una autenticación positiva de la entidad, puede producirse un rechazo o la finalización de la conexión, además de una entrada en el programa de auditoria de seguridad y un informe al centro de gestión de la seguridad. La selección de técnicas de autenticación dependerá de las circunstancias en que deben utilizarse, y, en la mayoría de los casos, deben emplearse junto con sellos de tiempo y de secuencia de los mensajes de autenticación (para evitar el reenvío de estos mensajes), la utilización de protocolos con fase de saludo (*handshake*) de dos o tres vías (para la autenticación unilateral y la autenticación mutua, respectivamente) y servicios de no repudio.

- *Sistemas de control de acceso*. El control de acceso a los recursos (es decir, el control sobre quién puede realizar qué operaciones sobre cuáles recursos) está relacionado con el concepto de protección de los sistemas. En general, existen dos perspectivas básicas para enfocar la protección de un sistema:

    - *Acceso discrecional*. Los sistemas que pertenecen a esta categoría se caracterizan porque el poseedor del objeto o recurso (*owner*) puede libremente conceder o denegar el acceso al mismo a cualquier usuario. Por tanto, una política discrecional está constituida por reglas de seguridad que afectan individualmente a cada usuario (o incluso a grupos de usuarios). Implementaciones concretas de este tipo de sistemas son las listas de control de acceso (*ACL*, *Access Control List*) o listas de capacidades.

    - *Acceso no discrecional*. En este tipo de sistemas el acceso a un objeto puede concederse o denegarse atendiendo al nivel de confidencialidad de la información (de acuerdo a una determinada clasificación) y la credencial que posea el usuario. Por lo tanto, una política no discrecional impone reglas de seguridad obligatorias para todos los usuarios.

  Un ejemplo de sistema de control de acceso a nivel de red, lo constituyen los cortafuegos (*firewalls*). Básicamente, los cortafuegos son sistemas que controlan el tráfico dentro de las redes canalizando el acceso al exterior de la red de la organización a través de un único punto. De esta forma, es posible analizar dónde se originan los paquetes transmitidos, que se pueden o no dejar atravesar el cortafuegos dependiendo del origen de los mismos, del destino, etc. Los cortafuegos pueden tener distintas formas: filtrador de paquetes, cortafuegos a nivel de circuitos y a nivel de aplicación.

Conviene resaltar que todos los mecanismos poseen tres componentes principales que los caracterizan:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, generación de resúmenes y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.