CAPÍTULO 1
CONCEPTOS BÁSICOS

1.1 SEGURIDAD Y REDES

Un sistema informático se compone de 5 elementos: hardware, software, datos, memoria y usuarios.

De estos componentes cualquiera puede convertirse en un objetivo para el delincuente informático. Con estas opciones para poder atacar algún sistema, se dificulta el análisis de riesgos y ofrece la ventaja de aplicar al delincuente la filosofía del punto más débil, lo que significa, atacar al sistema por su punto más vulnerable. Por lo tanto, de cara a la protección del sistema, será necesario considerar por igual a los elementos antes citados como vulnerables de un ataque.

1.1.1 Principios de la Seguridad Informática

La filosofía del punto más débil da lugar al primero de los tres Principios de la Seguridad Informática conocido como Principio del Acceso más Fácil. Los tres puntos de los Principios de la Seguridad Informática son:

- Principio del Acceso más fácil.
- Principio de la Caducidad de la Información.
- Principio de la Eficiencia.

- Principio del Acceso más fácil.

"El intruso al sistema utilizará cualquier artilugio o mecanismo que haga más fácil su acceso al sistema y posterior ataque."

Si se afirma que todo sistema informático presenta vulnerabilidades o debilidades en la seguridad de un sistema, aparecen tres preguntas básicas:

a) ¿De qué forma se manifiestan estas debilidades?
b) ¿Cómo se pueden clasificar las amenazas?
c) ¿Qué medidas de control se deben utilizar?

Dando solución a la primera cuestión; las debilidades de todo sistema informático se pueden agrupar en función de los problemas que ocasionan debido a la exposición, vulnerabilidades, ataques y amenazas.

La exposición se refiere a la posible pérdida o daño en el sistema debido a modificación, extravío de datos o acceso no autorizado al sistema. La vulnerabilidad es el punto débil del sistema que, si se traspasa, produce los efectos nocivos indicados. Un ataque es el hecho de la intromisión con daño manifiesto al sistema y, por último, las amenazas consisten en desastres naturales, errores humanos, fallos de hardware y software, sean fortuitos o voluntarios.

En cuanto a la segunda pregunta, dado que los objetivos principales de ataque son el hardware, el software y los datos, se clasifican las amenazas en cuatro tipos: amenazas de interrupción, intercepción, modificación y generación de la información en general.

Los objetivos amenazados (hardware, software, datos) pueden caracterizarse como un flujo (información, servicio, programas, datos, etc.). Si éste es el caso, una representación visual de cada una de estas amenazas se pueden observar en la Figura 1-1.

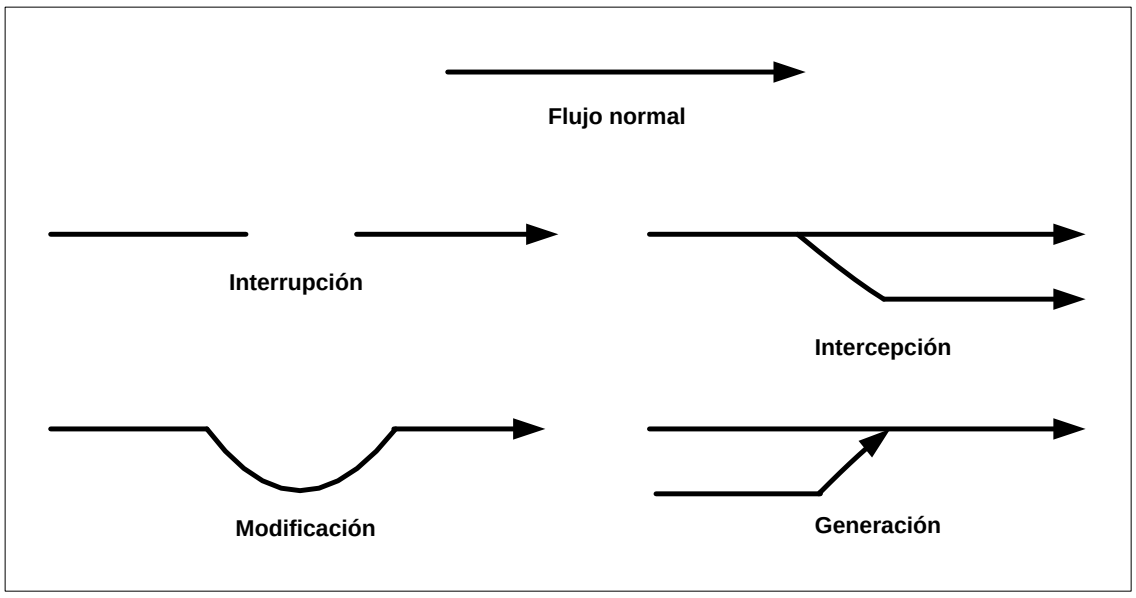

Figura 1-1. Representación gráfica de amenazas.

A continuación se detalla el alcance de cada una de éstas amenazas:

Interrupción:

Se produce cuando un punto del sistema se daña, pierde o deja de funcionar. La detección de este problema es inmediata, tanto por el sistema como por el usuario. Como ejemplos de interrupción son la destrucción maliciosa del hardware, borrado de programas y/o datos, fallos del sistema operativo, etc.

Intercepción:

Es el acceso a la información por parte de personas no autorizadas. Su detección resulta difícil dado que no deja huellas. Como ejemplos de intercepción son las copias ilícitas de programas y la escucha de una línea de datos.

Modificación:

Se produce una amenaza de modificación cuando alguien no autorizado accede al sistema y cambia el entorno para su beneficio. Dependiendo de las circunstancias puede resultar difícil de detectar, siendo ejemplos típicos los de modificación de una base de datos y los de hardware, aunque éste último es más sofisticado y menos frecuentes.

Generación:

Contempla la creación de nuevos objetivos dentro del sistema informático, tales como añadir transacciones específicas de red o registros a una base de datos. Su detección resulta difícil y en muchos casos se trata de un delito de falsificación.

- Principio de la Caducidad de la Información.

"Los datos deben protegerse sólo hasta que pierdan su valor."

En función de la caducidad de la información, se puede pensar en minutos, horas, días o años el tiempo en que se debe mantener la confidencialidad de los datos. Por ejemplo, no tendrán igual tratamiento los datos sobre un censo electoral que los de un desarrollo de un nuevo prototipo de software.

Cabe aclarar que este principio de la caducidad forzará a diseñar algoritmos criptográficos que cumplan con una determinada fortaleza al criptoanálisis (acción de

romper de forma ilegal un mensaje cifrado), en función del tiempo que se desee mantener en secreto la información.

Conociendo las debilidades y clasificando las amenazas, sólo resta decidir qué medidas de control se pueden implementar para proteger al sistema y a la información allí almacenada. Ello conlleva diversas acciones y procedimientos (planes de contingencia, controles de acceso, niveles de seguridad, etc.), así como el uso de dispositivos físicos específicos.

Para defenderse frente a estas amenazas se deben crear métodos de control que preserven el supuesto secreto asociado a la información, el acceso a esos datos solamente a las personas autorizadas y, por último, que tales datos estén disponibles a dicho usuario cuando éste lo desee. Estos tres aspectos darán lugar a los tres elementos básicos de la seguridad informática conocidos como confidencialidad, integridad y disponibilidad de la información.

En cuanto a los sistemas de control, éstos pueden ser mediante hardware, a través del uso de dispositivos que limiten físicamente el acceso a un programa, aplicación o datos; mediante software directo, los relacionados con el desarrollo de los sistemas operativos y programas que contemplan la protección de archivos, directorios, definición de niveles de usuarios, etc., y por último, el software de aplicación para el cifrado de la información.

- Principio de la eficiencia.

"Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio."

El decir que sean efectivas significa que cuando sean invocadas por un programa o por el usuario, funcionen perfectamente, lo que se puede asociar al hecho de estar en el lugar y momento oportunos. En cuanto a la eficiencia, se refiere a indicar que debe funcionar sin producir trastornos ni fallos al sistema informático, en términos de consumo de tiempo, ocupación de espacio de memoria o deficiente interfaz hombre/máquina. En resumen, que funcione y lo haga bien, optimizando el uso de recursos.

Todo esto lleva a la afirmación de que un buen sistema de seguridad es aquel que contempla controles eficaces y no obstante, pasa desapercibido por el sistema informático y por sus usuarios. [1]

1.1.2 Servicios de Seguridad

Un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio. [2]

Anteriormente se mencionaron tres elementos en los que se basa la seguridad informática, entendida ésta como seguridad lógica. Estos elementos son la confidencialidad, integridad y disponibilidad.

La confidencialidad de la información significa que los componentes del sistema son accesibles solamente por aquellos usuarios autorizados. La forma de acceder a estos datos puede ser mediante la lectura y observación de los mismos, su impresión, así como el simple conocimiento de su existencia. Si un documento es confidencial, se supone que existe un transmisor y uno o varios receptores autorizados y sólo ellos deberían tener acceso a dicho documento, es decir un secreto compartido.

Con respecto a la integridad, entendemos ésta como el hecho de que los componentes del sistema no sean modificados en la transición de la información. Esta modificación puede ser por medio de la escritura, cambios de datos, modificación de estatus, borrado y creación de nuevos objetos.

La disponibilidad indica que aquellos usuarios autorizados deben tener disponibles los componentes del sistema cuando así lo deseen y tantas veces como sea necesario.

Adicionalmente a estos tres servicios de seguridad se deben considerar los servicios de seguridad de no repudio, control de acceso y autenticación. Donde el

servicio de seguridad de la autenticación será el tema principal para la realización de esta tesis.

Se le conoce al servicio de seguridad de no repudio, como aquel que previene a los emisores o a los receptores de negar un mensaje transmitido. Cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor. Esto es, el no repudio ofrece protección a un usuario frente a otro usuario que niegue, posteriormente, haber realizado cierta comunicación o recepción de un mensaje enviado.

El control de acceso se refiere al mantener controlado el acceso a un medio de información ya sea a través de un dispositivo pasivo tal como una puerta cerrada o a través de un dispositivo activo como lo puede ser un monitor. Un monitor de control de acceso determina qué usuario está autorizado para usar un recurso de manera requerida. Antes de otorgar el acceso, el monitor puede validar la identidad del usuario.

La autenticación es el servicio de seguridad referente al "verificar" la identidad. En la vida diaria generalmente la autenticación se hace de manera informal y, en ocasiones, sin pensarlo. Todos inconscientemente autenticamos gente, compañías y ubicaciones todo el tiempo.

Por ejemplo, cuando se asiste a casa, autentica el hogar comparándolo con la memoria. Si se visita el hogar de un amigo, se verifica que está en la ubicación correcta comprobando la dirección dada por la calle y el número sobre la casa. Cuando se entra a una sucursal de un banco, lo autentica por su logotipo y colores.

La forma más popular de autenticación individual es una firma. Una firma se usa para autenticar al titular de la cuenta en el banco, para comprometer a una persona para alojarse en un hotel y para autenticar al titular de la tarjeta de crédito al realizar alguna compra. La firma se usa no solamente para autenticar la identidad, sino también para dar autorización.

El servicio de autenticación trata de asegurar que una comunicación sea auténtica. En el caso de un sólo mensaje como una señal de alarma o una advertencia, la función del servicio de autenticación asegura al receptor que el mensaje proviene de la fuente que éste espera que provenga.

En el caso de una interacción en curso como la conexión de una terminal a un anfitrión, dos aspectos son envueltos:

- Al momento en el que la conexión se inicia, el servicio verifica que las dos entidades sean auténticas (esto significa que cada entidad es en realidad la que se supone que debe ser).
- El servicio debe asegurar que la conexión no pueda ser interferida por un tercer individuo que pueda enmascararse como una de las dos entidades legítimas con el único propósito de realizar una transmisión o recepción no autorizada.

La autenticación es utilizada para proporcionar una prueba al sistema de que en realidad se es la entidad que se pretende ser. El sistema verifica la información que alguien provee contra la información que el sistema sabe sobre esa persona.

La autenticación es realizada principalmente a través de:

- Algo que se sabe: una contraseña o un número personal de identificación, es algo que se sabe. Cuando se le provee al sistema, éste lo verifica contra la copia que está almacenada en el sistema para determinar si la autenticación es exitosa o no.
- Algo que se tiene: una tarjeta o un pasaporte es un ejemplo de algo que se tiene, lo cual es utilizado por el sistema para verificar la identidad.
- Algo que se es: la voz, la retina, la imagen del rostro o una huella digital pueden identificar de quién se trata y pueden ser utilizadas en el proceso de autenticación. [2]

Por lo tanto, los servicios de seguridad que se mencionaron:

- Confidencialidad
- Integridad
- Disponibilidad
- No repudio

- Control de Acceso
- Autenticación

Si se cumplen completamente estos seis servicios se considera que los datos en una red de datos están protegidos y seguros.

1.1.3 Autenticación, Autorización y Auditoría (Contabilidad)

Una parte importante de la seguridad de la red es la autenticación, autorización y auditoría, conocidas colectivamente como la AAA (Authentication, Authorization and Accounting). AAA es un marco, en el que un administrador puede mantener el control de acceso sobre los dispositivos de red.

AAA cubre control de acceso sobre routers, switches, firewalls, servidores, etc. Cualquier dispositivo de red que no sea una estación de trabajo y que permite el acceso remoto, puede caer bajo las políticas AAA. AAA no es un protocolo en sí mismo, sino que es un conjunto de directrices promovidas por The Internet Engineering Task Force (IETF) que describe cómo deben comportarse los protocolos de acceso a optimizar sus beneficios de la seguridad.

Los protocolos más utilizados asociados a la AAA son Kerberos, Remote Authentication Dial-In User Service (RADIUS) y la terminal de acceso de controlador de sistema de control de acceso+ (TACACS+, Terminal Access Controller Access Control System+).

Al proporcionar un marco para el control de acceso, la AAA ofrece al administrador de red una forma de aplicar una política uniforme en todos los dispositivos de red. Este tipo de estándar de la política tiene dos ventajas: provee a un administrador de red la capacidad de centralizar toda la información contable, y crea un nivel de acceso que pueden aplicarse uniformemente a través de la red.

La capa AAA, cuando es necesario en las redes, permite la mezcla de los diferentes tipos de autenticación, no sólo dentro de la red, sino también en la misma interfaz de red. AAA, como con cualquier buen modelo de seguridad, proporciona a un

administrador de red una gran flexibilidad. Se ajusta en torno a una red existente, en lugar de obligar a la red a entrar en un rígido modelo de seguridad.

En la Figura 1-2 se muestra cómo un modelo de auditoría AAA encajaría en una red. Los servicios AAA en general se encuentran en las máquinas remotas, de modo que si un dispositivo de red está comprometido y, por consiguiente, la validez de sus propios registros es cuestionable, hay un registro independiente de los tiempos de acceso y, posiblemente, los cambios realizados en el dispositivo.

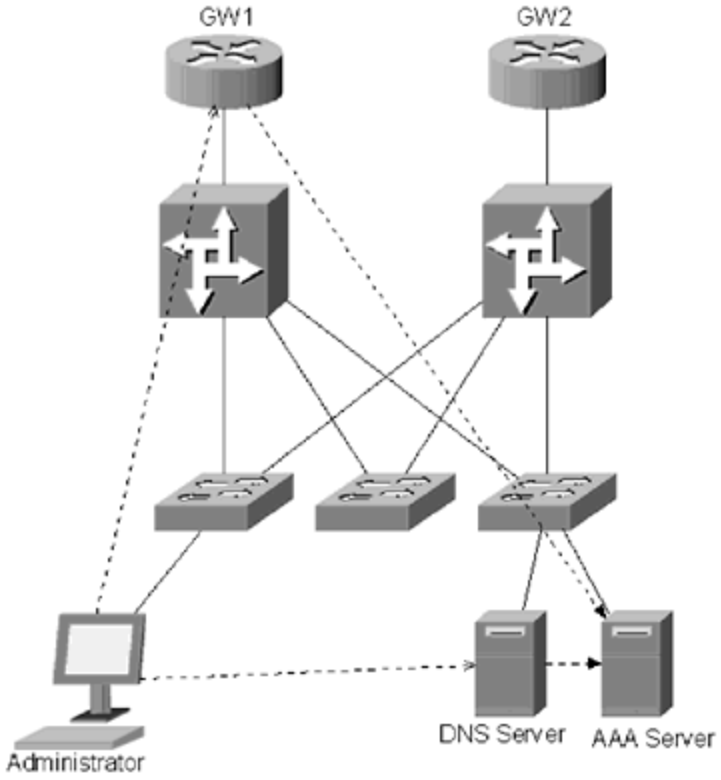

Figura 1-2. Una típica configuración de la red utilizando los servicios de la AAA.

La autenticación es el proceso en el que se identifica un usuario en un dispositivo. Esto incluye el nombre de usuario y la contraseña de proceso y el tipo de cifrado, si los hubiere, que se utiliza durante el proceso de autenticación. El objetivo de la autenticación es restringir el acceso a los dispositivos de red, por lo que tiene que producirse la autenticación antes de que un usuario tenga acceso a un dispositivo. La autenticación se define para cada interfaz. Múltiples formas de autenticación son compatibles con cada interfaz, sin embargo, una autenticación por defecto pueden ser asignada a todas las interfaces.

La autorización es el perfil de usuario. Es lo que determina el nivel de acceso, o lo servicios a los que un usuario tiene acceso. Autorización se puede definir en un par de maneras. Si la política de autorización para cada usuario va a ser coherente en toda la red, entonces la política de autorización se puede definir en el servidor AAA. Si la autorización de la política va a variar de un dispositivo a dispositivo, entonces las políticas de autorización se pueden definir sobre el dispositivo de red individual. Por ejemplo, un administrador de red puede querer definir distintas políticas para los routers y servidores, o un desarrollador web puede tener pleno acceso al servidor web, pero sólo un acceso limitado al servidor DNS. Las políticas de autorización no tienen que estar limitada para cada usuario. Se puede definir para cada grupo, con diferentes grupos con diferentes privilegios.

Controlar los registros, y qué privilegios se han registrado y cuando, no es suficiente. También tienen que ser capaces de controlar lo que hacen mientras está conectado, que es donde la auditoría es importante. La auditoría permite a un administrador de red controlar los tiempos de conexión de una cuenta, las órdenes emitidas mientras está conectado, los recursos utilizados, y los datos transferidos. Las características de la auditoría pueden añadir sobrecarga a la red, sin embargo, la información adicional puede ser de un valor incalculable cuando se trata de localizar, ya sea interno o externo un atacante como la contabilidad del servidor AAA tiene un registro completo de los movimientos realizados por un atacante.

1.1.4 Redes de datos

Una red de datos es un sistema de comunicación que permite a un número de sistemas y dispositivos comunicarse unos con otros [3]. La cual permite enviar y recibir mensajes entre cada uno de los usuarios, los mensajes pueden ser un mail, un documento, una imagen o cualquier forma de comunicación entre los mismos.

Es posible clasificar las redes por su escala [3]:

Local Area Network (LAN, Red de Área Local), son redes óptimas para un área geográfica moderada, como un campus de pocos kilómetros o algún edificio. Son utilizadas para conectar computadoras personales y estaciones de trabajo en oficinas,

sus restricciones se encuentran tanto en el número de usuarios que soportan como en el tiempo de transmisión que es conocido y limitado. Utiliza generalmente conexión mediante cable Ethernet o fibra óptica.

Metropolitan Area Network (MAN, Red de Área Metropolitana), son redes de tamaño medio que abarca una ciudad. Usualmente conectadas mediante cable coaxial o microondas.

Wide Area Network (WAN, Red de Área Amplia), son redes que se expanden en una gran área geográfica, generalmente un país o un continente. Estas contienen un conjunto de máquinas llamadas host, diseñadas para aplicaciones de usuarios. Los host se encuentran conectados en subredes, que se encargan de llevar los mensajes de un host a otro. En la mayoría de las redes de área amplia la subred está compuesta de líneas de transmisión y elementos de conmutación.

1.1.5 Diseño de redes: protocolos y capas

Un protocolo de red es un conjunto de reglas sobre el intercambio de comunicación en la red. Dos sistemas o usuarios que intercambian información deben tener un protocolo en común para tal efecto. Un protocolo determina el formato y la secuencia en la que los mensajes pasan de emisor a receptor, sin importar el medio o la forma con la que se haga la comunicación [3].

Para reducir la complejidad del diseño de redes, la mayor está organizada como una pila de capas o niveles independientes. El propósito de una capa de protocolos es proveer servicios a la capa superior. Un conjunto de capas y protocolos se conoce como arquitectura de red.

El modelo de referencia Open Systems Inteconnection (OSI, Interconexión de Sistemas Abiertos) es una propuesta desarrollada por la International Organization for Standardization (ISO, Organización Internacional de Estándares) para la estandarización de la comunicación entre sistemas, su estructura se utiliza para mostrar cada una de las

funciones de cada capa y tener un estándar a seguir en el desarrollo de aplicaciones de comunicación.

La seguridad, no se refiere o aplica a una sola capa del modelo, debido a que es posible realizar una implementación de seguridad en cada una de ellas, al revisar cada capa (Figura 1-3) es posible indagar que cada una tiene cientos de vulnerabilidades, por ejemplo, es visible que si una de las capas es vulnerada, las comunicaciones están en peligro sin que las otras capas sean conscientes del problema, por lo que es necesario llevar a cabo todas las posibles soluciones que se han desarrollado tanto de protocolos y aplicaciones, como de hardware y software para tratar de mantener segura la información viaja a través de la red.

Figura 1-3. El modelo de referencia OSI.

A continuación se dará una breve explicación de las capas en que se centrará el análisis [3]:

La capa física consiste en estándares que describen el orden de los bits, las tasas de transmisión de bits, tipos de conectores y otras especificaciones. La información en esta capa es transmitida en formato binario.

La capa de enlace de datos de manera general esta capa se encarga de transformar los bits puros recibidos del canal de comunicación y llevarlos a la capa de red sin errores. Generalmente esto se resuelve mediante la fragmentación de la información en tramas enviadas secuencialmente y recibiendo una confirmación de recepción. De la misma manera es posible controlar en esta capa la no saturación de los datos enviados.

La Institute of Electrical and Electronics Engineers (IEEE, Instituto de Ingenieros Eléctricos y Electrónicos) divide la capa de enlace de datos en dos subcapas: subcapa Logical Link Control (LLC, Control de Enlace Lógico) y la subcapa Medium Acces Control (MAC, Control de Acceso al Medio).

1.1.6 Seguridad en capas

Un sólo mecanismo no puede ser utilizado para proteger una red. Para proteger la infraestructura debe aplicarse la seguridad en capas, también conocida como defensa profunda [5]. La idea es crear varios sistemas, de tal forma que si existe un fallo en alguno de ellos no se convierte en una vulnerabilidad, pero es interceptado en la siguiente capa. Adicionalmente la vulnerabilidad puede ser limitada y controlada en la capa afectada debido a la seguridad aplicada a diferentes niveles. La seguridad en capas es el método preferido y más escalable para proteger una red.

1.1.7 Seguridad en redes

En los primeros días de las redes, el administrador de la red por lo general tenía un estricto control sobre la conexión remota de los sistemas. En la actualidad, la proliferación de las redes interconectadas y el fácil acceso remoto e intercambio de recursos, resulta casi imposible identificar y confiar en todos los puntos de acceso de un sistema.

La seguridad en redes es definida (por la United States National Security Agency, NSA, Agencia de Seguridad Nacional de los Estados Unidos) como la protección de las redes y sus servicios de la modificación, destrucción o divulgación no autorizada, asegurándose que la red trabaje correctamente sus funciones críticas y sin efectos secundarios perjudiciales [4].

Hay una serie de estrategias diferentes para lograr la seguridad en un entorno de red. La elección de cuáles y cuántas estrategias se utilizaran depende en gran medida del

tipo y alcance de la red, el nivel de confianza de los usuarios y el valor de la información transmitida.

La seguridad en redes por lo tanto es un sistema, no es un firewall, un detector de intrusos, una red privada virtual, no es la autorización, la autenticación y la auditoría. La seguridad son todas las soluciones que existen en el mercado para la protección de los servicios de red [4].

Con ambas referencias, es posible entender que un sistema de seguridad de redes es una colección de dispositivos y tecnologías conectadas a la red, aunadas a buenas prácticas que trabajan complementariamente para proporcionar seguridad a los activos informáticos.

1.1.7.1 Estándares de Seguridad en Redes

La IEEE ha desarrollado un conjunto de normas, conocidas como el estándar 802, principalmente para redes de área local [4]. Los primeros estándares 802, que van del 802.1 al 802.10, básicamente abordan las dos capas más bajas del modelo OSI. El 802.10 es un estándar para la interoperabilidad de la seguridad LAN, conocido como Standard for Interoperable LAN Security (SILS), que está orientado al intercambio de datos en redes.

El estándar X.400 desarrollado por la ISO y Consultative Committee for International Telegraphy and Telephony (CCITT, Comité Consultivo de Telegrafía y Telefonía Internacional), conocido actualmente como International Telecommunication Union (ITU-T, Unión Internacional de Telecomunicaciones), es orientando al modelo OSI para mensajes, que incluyen normas para la seguridad de la mensajería [4].

El estándar X.500 también elaborado por la ISO y CCITT, son las normas elaboradas para la asignación de nombres [4]. Permiten a los usuarios y programadores identificar un objeto (archivo, disco, etc.) sin saber la ubicación del objeto en una red o la ruta de acceso necesaria para alcanzarla. Incluye normas para garantizar la autenticación y nomenclatura segura. La mayoría de los servicios actuales de autenticación dependen de un sistema de parámetros definidos en el X.500.

El estándar X.500 es un sistema global, en la mayoría de los casos el directorio X.500 es generalmente accesible utilizando una herramienta llamada Lightweight Directory Access Protocol (LDAP, Protocolo Ligero de Acceso a Directorios).

Ejemplo de una red de datos [6].

A continuación se mostrara un ejemplo de una típica red corporativa para una empresa de 100 personas. Esta red es bastante insegura. Por supuesto, no hay un modelo de seguridad correcta. Las necesidades en materia de seguridad varían de una compañía a otra, pero es más fácil para los administradores de red, visualizar como corregir y detectar deficiencias para crear mejores métodos.

La infraestructura de red.

Para el ejemplo de la Figura 1-4 es simple: un router conectado a un firewall que tiene tres interfaces, una pública al router y dos privadas, una a la red de los empleados y otra a los servidores.

El conjunto de reglas utilizado por este firewall es muy simple. No es permitido el tráfico hacia la red de los empleados. Todo el tráfico es permitido hacia la red de los servidores. Las reglas a la red de los servidores son ligeras debido a que es necesario tener todos los puertos abiertos.

La compañía utiliza una infraestructura de red Transmmision Control Protocol/Internet Protocol (TCP/IP, Protocolo de Control de Transmisión/Protocolo de Internet), pero no se han realizado auditorías para saber que otros protocolos están funcionando en las máquinas. Utilizan el bloque de red 10.10.10.0 255.255.255.0 (clase C). Las direcciones IP han sido asignadas sin subredes.

Finalmente, todas las máquinas conectadas a un switch utilizan la Virtual Local Area Network (VLAN, Red de Área Local Virtual) por default, ya que los administradores no han asignado diferentes VLAN a los puertos.

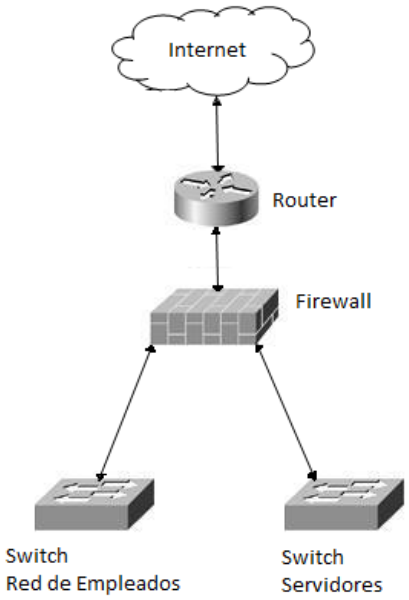

Figura 1-4. Infraestructura de red.

Los Servidores.

Consta de cinco servidores, todos excepto dos, realizan funciones únicas (Fig. 1-5). El servidor de archivos también hace las tareas de un servidor acceso remoto que permite a los empleado entrar a la red desde casa, mientras el controlador de dominio hace a la vez de servidor de monitoreo.

El servidor de archivos, Exchange y el controlador de dominio funcionan bajo Windows NT, con Service Pack 4 instalado. El servidor de dominio y web se encuentran en Red Hat Linux 6.2.

Las cuentas son creadas, según las necesidades, y no han sido auditadas.

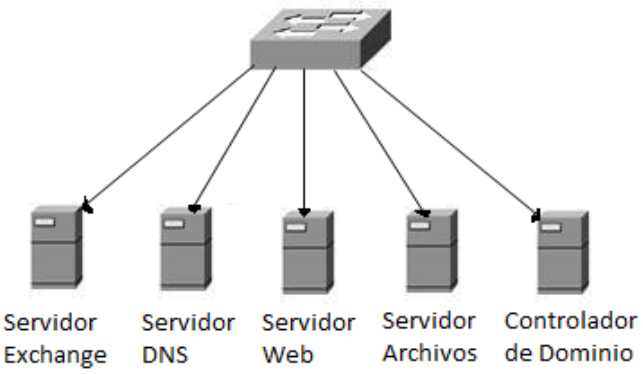

Figura 1-5. Servidores.

La red de los empleados.

Varios grupos de empleados, como recursos humanos o contabilidad, están conectados vía hub a switch de la red (Fig. 1-6). Estos empleados utilizan una combinación de versiones de Windows. De nueva cuenta no hay auditorías o políticas que limiten el tipo de equipos que se unen a la red.

A todos los equipos en red se les asigna una dirección IP por el controlador de dominio cuando inician sesión en la red.

La empresa utiliza red inalámbrica sólo en un par de salones de conferencia, permitiendo a todo equipo con tecnología inalámbrica conectarse a la red.

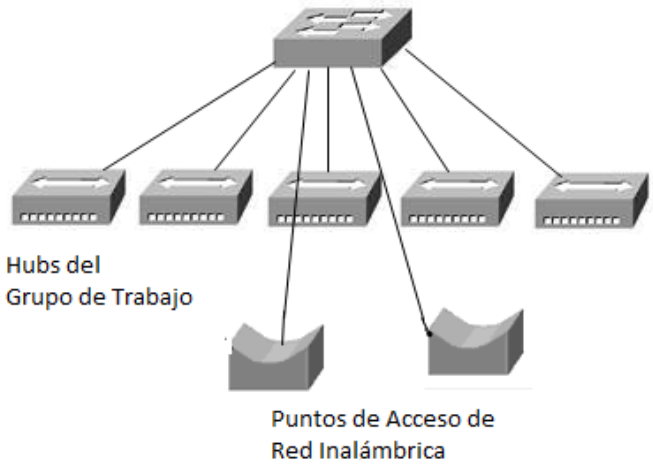

Figura 1-6. Red de empleados.

1.2 CRIPTOGRAFÍA

Criptografía (Etimología de ocultar + escritura) es el arte, técnica o ciencia que permite proteger a la información por medio de la aplicación de un cifrado. Esta sólo puedes ser descifrada por el remitente autorizado. La criptografía da lugar al criptólogo y al criptoanalista, el criptólogo es la persona que trabaja en nombre de un transmisor o receptor no autorizado y cuya función básica es la de crear algoritmos de cifrado y descifrado, mientras el criptoanalista es la persona que trabaja en nombre de un transmisor o receptor no autorizado y cuya función básica es la de romper códigos y textos cifrados para recuperar de forma ilegítima la información allí contenida, utiliza el criptoanálisis como herramienta para descriptar.

Se le conoce a la Criptología como la ciencia que estudia e investiga todo lo concerniente a la criptografía. Esto da lugar al cifrado y descifrado, donde el cifrado es la técnica por la cual, a través de un algoritmo, se modifica o altera la representación de un texto en claro convirtiéndolo en un criptograma de forma que su intercepción por extraños no entregue información alguna del mensaje original y el descifrado es la técnica por la cual a través de un algoritmo, generalmente el inverso del cifrado, un receptor legítimo puede recuperar la información contenida en el criptograma.

Alternativamente existe la Codificación, que es la técnica de cifrar por medio de códigos, no por algoritmos de cifrado. Y la Decodificación, que es la recuperación de la información codificada aplicando una relación directa entre código palabra.

En el proceso de la criptografía se obtiene el Criptograma, el cual es el documento obtenido al cifrar un texto en claro. La representación o alfabeto del criptograma puede ser igual o distinta a la del texto en claro. De modo contrario el texto en claro es el documento original o mensaje que se desea enviar a uno o más destinatarios o bien, almacenar en forma criptografiada.

Dentro de la Criptografía además se emplea el concepto de Clave privada, la cual es la clave secreta utilizada para cifrar un mensaje y cuyo secreto mantiene la inmunidad del sistema. Esto da lugar a criptosistemas de clave secreta. Por otro lado la Clave pública es la clave utilizada en criptosistemas, conjuntamente con una clave privada o secreta, de forma que se cifra con una de ellas y se descifra con la otra. La inmunidad de estos sistemas se basa en el hecho de que, incluso conociendo el algoritmo o transformación y la clave para cifrar, resulta extremadamente difícil romper o descriptar un criptograma sin conocer la segunda clave.

Estos tipos claves dan lugar a la Sustitución, que es la técnica criptográfica que consiste en sustituir un carácter del texto en clave por otro en el texto cifrado. Existen dos tipos de sustitución; la Sustitución monoalfabética y la Sustitución polialfabética. La Sustitución monoalfabética es el cifrado que sustituye cada carácter del texto en clave por otro carácter único en el criptograma, usando un único alfabeto. La Sustitución polialfabética es el cifrado que, mediante una clave, sustituye los caracteres

del texto en claro por otro carácter en el texto cifrado, utilizando para ello más de un alfabeto. Adicional a estos cifrados existe la Transposición, el Cifrador de Bloques y Cifrador de Flujo. La Transposición es la técnica de cifrado que consiste en reordenar un texto en claro (también se conoce como permutación), el Cifrador de Bloques es un sistema que decide previamente el mensaje en bloques de igual tamaño y que luego cifra con la misma clave y Cifrador de Flujo es un Sistema que cifra el mensaje carácter a carácter (o bit a bit) mediante el elemento i-ésimo del flujo de una clave.

1.2.1 Criptografía Simétrica

La criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado ampliamente utilizados tienen estas propiedades, por ejemplo el algoritmo GPG en sistemas *GNU*.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad; para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio. En realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72, 057, 594, 037, 927, 936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

1.2.1.1 Criptosistemas de Clave Secreta

También conocidos como de clase única o criptosistemas simétricos, basan su fortaleza en el secreto de la clave k (Figura 1-7). Si se llega a descubrir esta clave secreta, resultaría fácil por lo menos en la teoría obtener las funciones de cifrado y descifrado. La clave k es secreta y compartida por los dos usuarios, el transmisor y el receptor. Se verá un poco más a detalle cómo se aseguran en estos sistemas la confidencialidad y la integridad.

Puesto que solamente el usuario receptor autorizado conocerá la clave con la que ha cifrado el mensaje el usuario transmisor, se asegura de esta forma la confidencialidad: otro usuario no autorizado y que por tanto desconoce la clave, no podrá interpretar el criptograma. Por su parte, dado que sólo el usuario transmisor auténtico está en conocimiento de la clave secreta, el receptor puede estar seguro de que no se trata de un impostor y, por lo tanto, se confirma la integridad de la información. En resumen, al ser la clave única, secreta y compartida por ambos usuarios, podemos afirmar que en los criptosistemas de clave secreta la confidencialidad y la integridad de la información se obtienen al mismo tiempo.

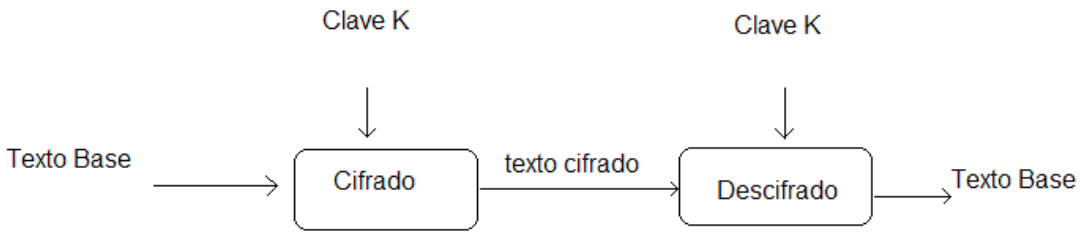

Figura 1-7. Criptosistema de clave secreta.

Aplicando las relaciones de transformación E_k y D_k, podemos representar el criptosistema como se indica en la Figura 1-8.

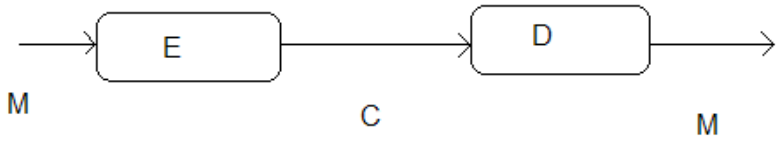

Figura 1-8.Transformaciones en un criptosistema de clave secreta.

Del esquema presentado en la Figura 1-8, se puede deducir las funciones de transformación que tienen lugar un criptosistema de clave secreta:

$$C=E(M)$$

$$M=D(C)$$

$$M = D(E(M))$$

Si la clave es K: $C = E(K, M))$

Luego $M = C(K, E(K, M))$

Representando a la clave de cifrado como K_E y a la clave de descifrado por K_D, ambas son inversas entre sí módulo n. La ecuación anterior sigue siendo válida y se transforma en:

$$M = D(K_D, E(K_E, M))$$

El primer conjunto de ecuaciones se corresponde con los criptosistemas clásicos sin clave como, por ejemplo el cifrado del César, en el que el criptograma se obtiene

simplemente aplicando un desplazamiento de k lugares a la derecha (k = 3 en este caso) en módulo n a cada uno de los caracteres del texto en claro.

Ejemplo 1-1: Usando la función indicada del cifrado del César, se pide:

a) Encontrar el alfabeto de cifrado y luego cifrar el siguiente Mensaje M = PELIGRO.

b) Repetir el punto anterior usando ahora como clave la cadena MURCIELAGO

Solución: Los alfabetos de cifrado y sus correspondientes criptogramas serán los que se indican a continuación:

a) A B C D E F G H I J K M L N Ñ O P Q R S T U V W X Y Z

Alfabeto cifrado: D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

M = PELIGRO => C = SHÑLJUR

b) A B C D E F G H I J K M L N Ñ O P Q R S T U V W X Y Z

Alfabeto cifrado: M U R C I E L A G O D F H J K N Ñ P Q S T V W X Y Z B

M = PELIGRO => C = ÑIFGLQN

Del ejemplo anterior se puede apreciar la diferencia entre utilizar solamente un algoritmo (en ese caso el del César) para cifrar y usar, además, una verdadera clave. Resulta evidente que en el caso de utilizar una clave existe una difusión mayor entre los elementos del alfabeto y, por consiguiente, dificulta en cierta forma el ataque al criptograma. Veremos a continuación cómo puede conseguirse la confidencialidad y la integridad en estos sistemas mediante un análisis genérico.

Para alcanzar la confidencialidad deberá ser imposible entonces para un intruso determinar D_k a partir del criptograma C, incluso en el caso extremo que conozca por algún medio el mensaje claro M. De esto se concluye que para mantener el secreto, esto es, que no se pueda determinar de forma ilegal M partir de C, la condición necesaria es que D_k se mantenga en secreto.

En otras palabras, para alcanzar el objetivo de la confidencialidad deberá cumplirse que:

a) El criptoanalista no podrá determinar sistemáticamente la operación de descifrado: esto es, no podrá descifrar C u otro texto cifrado bajo la transformación E_k.

b) El criptoanalista no podrá determinar sistemáticamente el texto en claro sin contar con la transformación de descifrado.

Estos dos requisitos, que se entremezclan, deberán mantenerse independientemente de la longitud y del número de mensajes interceptados. Esto es, no por tener un criptograma más largo o, por el contrario, contar con una gran cantidad de criptogramas, será más fácil el trabajo de un criptoanalista. Ahora bien, siempre hay que contar con el factor suerte de forma que, aunque sea muy difícil determinar D_k y requiera de una gran cantidad de cálculos, por un acierto genial el criptoanalista logre determinarla sin más. Se debe observar, no obstante, que si sólo se desea mantener el secreto de la información, bastará con mantener en secreto la función de descifrado, con lo cual podríamos hacer pública la función de cifrado E_k, salvo que su conocimiento por parte de un extraño permitiera inferir la función D_k.

Si se profundiza ahora sobre el objetivo de la integridad o autenticidad de la información, ésta se logra si resulta imposible para un impostor enviar un mensaje haciéndose pasar por el transmisor legítimo. Esto es lo mismo que decir que sea imposible determinar la función E_k a partir del criptograma C, incluso si se conoce el mensaje en claro M. Por lo tanto, para que sea imposible encontrar de forma sistemática un criptograma C' tal que D_k (C') sea un texto base válido en el conjunto de los mensajes M, la función de cifrado E_k deberá ser secreta (Figura 1-9).

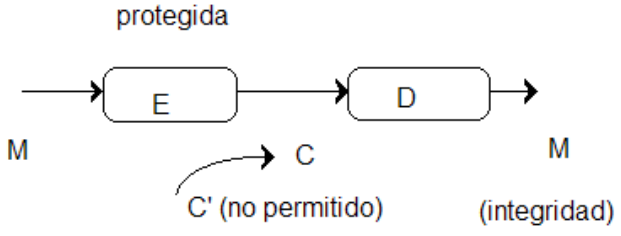

Figura 1-9. Integridad en un sistema de clave secreta.

En otras palabras, para alcanzar el objetivo de integridad deberá cumplirse que:

a) Debe ser computacionalmente imposible que un criptoanalista sistemáticamente determine la transformación de cifrado E_k a partir de C, aunque se conozca el texto en claro del mensaje M. Esto es, no podrá cifrar un texto en claro diferente M' y enviarlo como C' = E_k (M') al destinatario en vez de C.

b) Debe ser computacionalmente imposible que un criptoanalista encuentre de forma sistemática un texto cifrado C' tal que, al aplicarle la transformación D_k, obtenga un texto en claro válido en el espacio de mensajes M sin la transformación de cifrado.

De lo anterior se deduce que la función de cifrado E_k deberá estar protegida. No obstante, de forma similar al caso anterior de la confidencialidad, ahora podríamos hacer pública la función de descifrado si lo que nos interesa es únicamente preservar la autenticidad del mensaje. ¿Cómo se logra entonces que se cumplan ambos requisitos de seguridad, es decir, la confidencialidad y la integridad, en un sistema de clave secreta? La respuesta es obvia: protegiendo o haciendo secretas ambas funciones, la de cifrado y la de descifrado. De ahí que dado el secreto de la clave, en estos sistemas la confidencialidad y la integridad se obtienen de forma conjunta. No llegaremos a la misma conclusión en los sistemas de clave pública que se analizaran un poco más adelante en este mismo capítulo.

En resumen, la protección total en los sistemas de clave secreta se puede dar tal y como se muestra en la Figura 1-10.

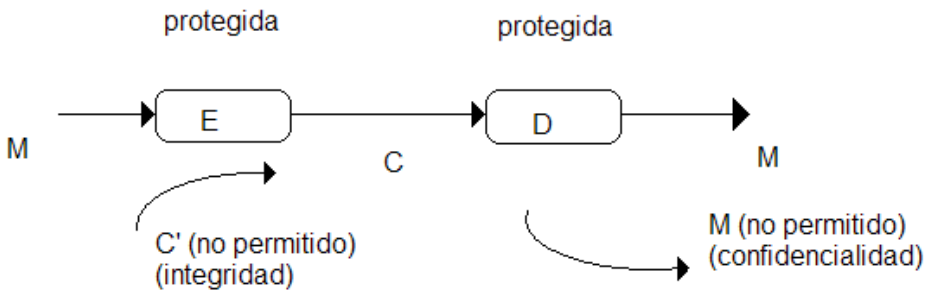

Figura 1-10. Integridad y confidencialidad en un sistema de clave secreta.

1.2.2 Criptografía Asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño de la clave del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave del tamaño de 80 bits, el atacante debe probar hasta 280-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

1.2.2.1 Criptosistemas de Clave Pública

Como se observó en el subtema anterior, al parecer los criptosistemas de clave secreta funcionan bien, pues sólo con mantener en secreto una clave, se asegura el secreto de la información y su autenticidad. Es más, muchos de ellos presentan una apreciable seguridad, siendo uno de los más conocidos y ampliamente utilizados en el mundo empresarial y de negocios el DES (Data Encryption Standard). Si esto es así, ¿Por qué plantearse entonces otro tipo de sistema conocido como de clave pública?

La respuesta a esta pregunta es muy sencilla aunque mucho más extensa que la que presentamos a continuación, no por ello menos válida.

Suponer que dos usuarios desean intercambiarse mensajes secretos y para ello deciden utilizar un sistema de cifrado de clave secreta; es esto es, eligen ambos una clave que sólo ellos conocen y mantienen en secreto. En este entorno, es evidente que ambas claves son iguales.

Suponer ahora que el grupo decide integrar a otro usuario, y deciden mantener las conversaciones secretas independientes de forma que, además de las dos claves anteriores, se crean dos claves más, para mantener comunicaciones independientes del tercer usuario con el primero y el segundo. Esto implica que el número de claves ha crecido de una a tres, mientras que el número de usuarios sólo ha aumentado en uno. Es fácil comprobar que si añadimos un cuarto participante en este grupo, el espacio de claves crecerá ahora hasta 6.

Por tanto no existe una relación lineal entre el número de usuarios del sistema y el número de claves secretas necesarias para conservar el secreto y la autenticidad de los mensajes que se intercambian.

Deduciendo que al aumentar el número de usuarios n, el número de claves secretas tiende a n^2. Por ese motivo, resulta impracticable para sistemas con muchos usuarios, básicamente por dos aspectos puntuales:

- Si no existe un control exhaustivo de las claves, pueden aparecer claves repetidas, lo que obviamente desvirtúa el concepto de secreto y autenticidad de todo sistema de cifrado.

- Por otra parte, al crecer de forma cuadrática el número de claves secretas, dificulta el trabajo del usuario que desea comunicarse con todos los demás, puesto que deberá conocer un gran número de claves diferentes, que al ser secretas tendría que tenerlas en mente y no en un archivo y menos en un listado.

Todo esto se complica aún más si se considera la tendencia actual de intercomunicación a través de redes mundiales. De ahí nace la necesidad de crear un criptosistema en el que el número de claves crezca en forma lineal con respecto al número de usuarios, sin por ello verse afectada la seguridad de la información que por él se transmite. Asimismo, al verse reducido el número de claves secretas, la gestión de las mismas se simplifica y el sistema es más económico.

La filosofía de un criptosistema de clave pública reside en que cada usuario dispone de dos claves, una de ellas de carácter privado (secreta) nombrado de forma genérica $u_i v$, y otra de carácter público que es $u_i b$. El subíndice i indica que dicha clave, privada o pública, pertenece al usuario i-ésimo. Las claves $u_i v$ y $u_i b$ serán inversos en el cuerpo o módulo en que trabaje el cifrador, en el sentido matemático.

La idea es que cada usuario cifre sus mensajes con una de las dos claves y los descifre con la otra, en función de que le interese bien conservar la confidencialidad, bien la integridad de su información, o bien ambas a la vez. El secreto del sistema está en que por mucho que los demás usuarios conozcan nuestra clave pública, les será computacionalmente imposible determinar nuestra clave privada. Ahora bien, no debemos perder de vista que el algoritmo de cifrado y descifrado es público; más aún, será muy sencillo.

A diferencia de los criptogramas de clave secreta, en los criptogramas de clave pública la confidencialidad y la integridad de la información se obtienen de forma separada. Por otra parte resulta obvio, que hemos solucionado el problema cuadrático del número de claves puesto que si un nuevo usuario j entra en el sistema el número de

claves simplemente crece en una unidad, que corresponde a su clave pública u_ib, ya que la clave privada u_iv es personal y no forma parte del sistema de claves.

A continuación y al igual que en los sistemas de clave secreta, realizaremos el análisis de las transformaciones de cifrado y descifrado que aseguran el secreto y la autenticidad en los sistemas de clave pública. Para una mayor sencillez en la explicación, supondremos una comunicación en que el usuario A envía un mensaje secreto a su amigo B por lo que las claves serán las siguientes:

- E_A es la operación con clave de cifrado de A y es pública.
- D_A es la operación con clave de descifrado de A y es privada.
- E_B es la operación con la clave de cifrado de B y es pública.
- D_B es la operación con la clave de descifrado de B y es privada.

Como se ha comentado, para lograr la confidencialidad, A envía el mensaje a B cifrándolo con la clave pública de B, es decir, E_B. Por su parte, B recibe el criptograma C y los descifra utilizando su clave privada D_B (Figura 1-11).

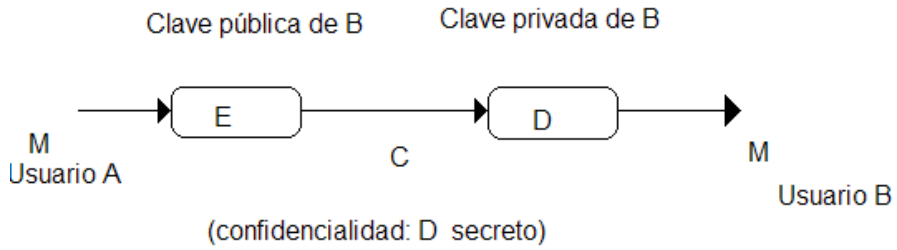

Figura 1-11. Confidencialidad en un sistema de clave pública.

$$C = E_B(M) \qquad \text{(operación de cifrado)}$$
$$M = D_B(C) = D_B(E_B(M)) \qquad \text{(operación de descifrado)}$$

Hay que observar que esta operación de cifrado sólo asegura el secreto; esto es que solamente el usuario a quien se dirige el mensaje podrá descifrarlo, pero no así la autenticidad. Cualquier otro usuario impostor A' podría hacerse pasar por el usuario A y enviar un mensaje M' al usuario B, en tanto que la clave pública de B la conoce todo el mundo.

Si el usuario A desea mantener la integridad de sus mensajes, esto es que nadie pueda hacerse pasar por él, entonces los cifrará con su clave privada D_A. El usuario B (o cualquier otro que pudiera leer el mensaje) lo podrá descifrar con la clave pública de A, es decir E_A (Figura 1-12).

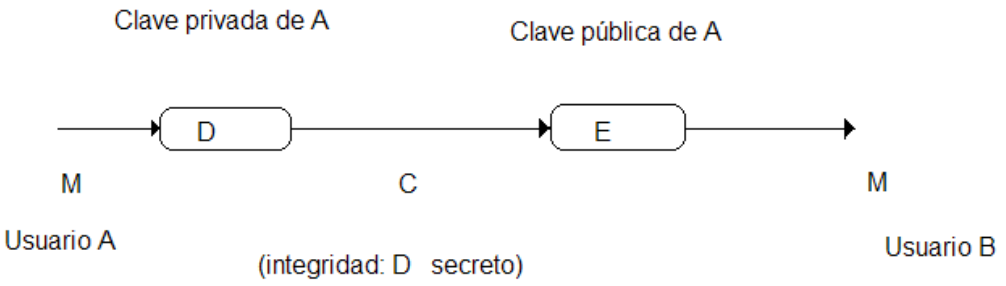

Figura 1-12. Integridad en un sistema de clave pública.

Las transformaciones aplicadas serán en este caso:

$C = D_A (M)$ (operación de cifrado)

$M = E_A(C) = E_A (D_A (M))$ (operación de cifrado)

Resulta claro que con esto se asegura la autenticidad de quien envía el mensaje, pero no así que dicho mensaje sea secreto. Como todo el mundo conoce la clave pública de A, dicho mensaje es también público. En este caso, y a diferencia de los criptogramas de clave secreta, estas dos características se obtienen por separado.

¿Cómo se puede entonces obtener para un mensaje cifrado con un sistema de clave pública la confidencialidad y la integridad? La respuesta: aplicando las dos operaciones anteriores tal y como se muestra en la Figura 1-13.

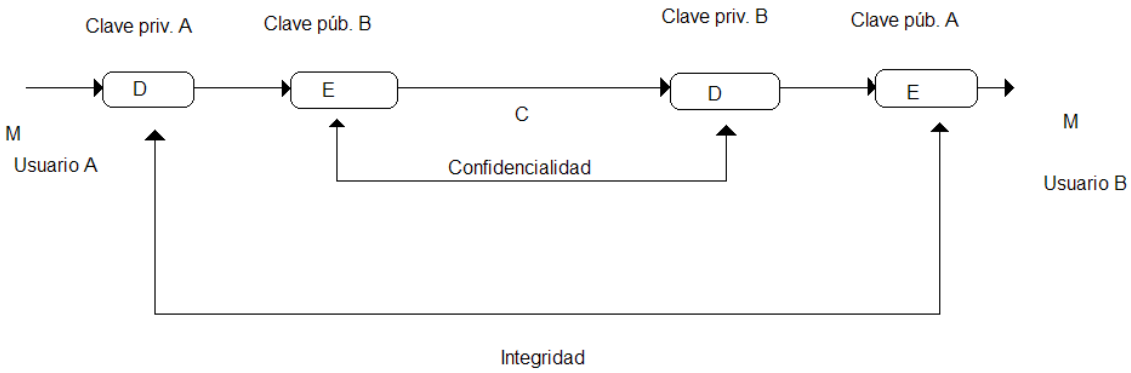

Figura 1-13. Confidencialidad e Integridad en un sistema de clave pública.

En este caso las transformaciones serán las siguientes:

$C = E_A (D_A (M))$ (operación de cifrado)

$M = E_A (D_B (C))$ (operación de descifrado)

De esta manera, se puede obtener un esquema criptográfico de clave pública que permite simultáneamente asegurar el secreto y la autenticidad del mensaje ampliamente conocido y que basa su fortaleza en la dificultad matemática que presenta factorizar números grandes.