Sistemas Operativos

Seguridad

Armando Arce, Escuela de Computación, arce@itcr.ac.cr

Tecnológico de Costa Rica

Seguridad

Los recursos informáticos deben protegerse frente a los accesos no autorizados, frente a la modificación o destrucción maliciosas y frente a la introducción accidental de incoherencias.

El problema de la seguridad

Se dice que un sistema es seguro si sus recursos se utilizan de la forma prevista y si se accede a ellos tal como se pretendía; en todas las circunstancias.

- Desafortunadamente, no es posible conseguir una seguridad total; a pesar de ello, se debe preveer mecanismos para hacer que los fallos de seguridad constituyan la excepción, en lugar de la norma.

Tipos de amenazas y ataques

Una amenaza es la posibilidad de que exista una violación de seguridad, como por ejemplo el descubrimiento de una vulnerabilidad, mientras que un ataque es un intento deliberado de romper la seguridad.

Tipos de amenazas y ataques

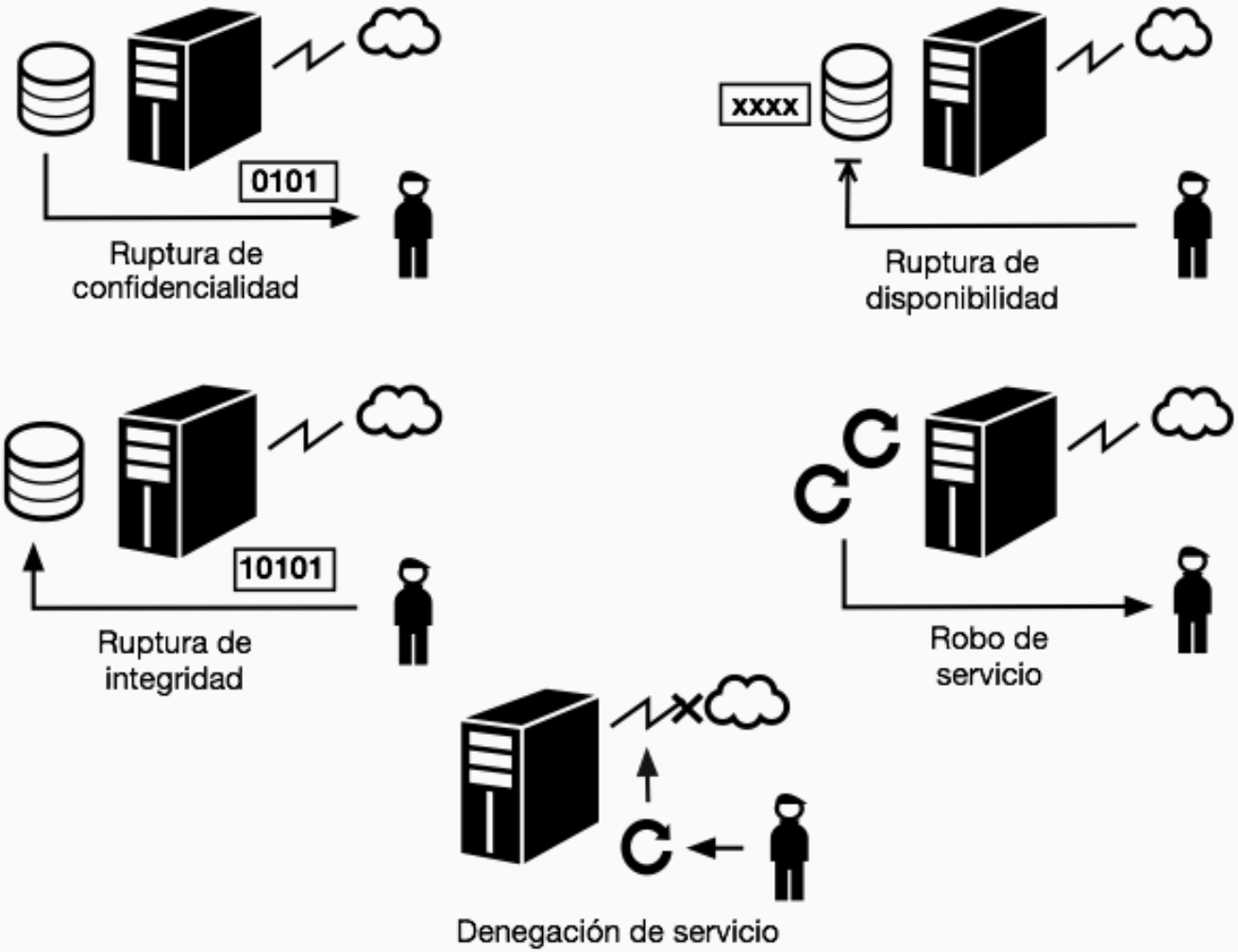

Figure 1:

Tipos de amenazas y ataques

La siguiente lista describe diversas formas de violaciones de seguridad tanto accidentales como maliciosas.

- Ruptura de la confidencialidad: Este tipo de violación implica la lectura no autorizada de determinados datos (o el robo de información), p.ej. números de tarjetas de crédito.
- Ruptura de la integridad: Implica la modificación no autorizada de los datos, p. ej. modificar el código fuente de una aplicación comercial.
- Ruptura de la disponibilidad: Consiste de la destrucción no autorizada de datos, p.ej. la sustitución de la página de entrada de un sitio web.
- Robo de servicio: Implica el uso no autorizado de recursos, p.ej. instalar de forma fraudulenta un servidor de archivos.
- Denegación de servicio: Consiste en impedir el uso legítimo de los recursos del sistema.

Métodos para romper la seguridad

Los atacantes utilizan diversos métodos estándar en sus intentos de romper la seguridad de los sistemas, entre ellos:

- mascarada,
- ataques de reproducción y
- ataque por interposición.

Métodos para romper la seguridad

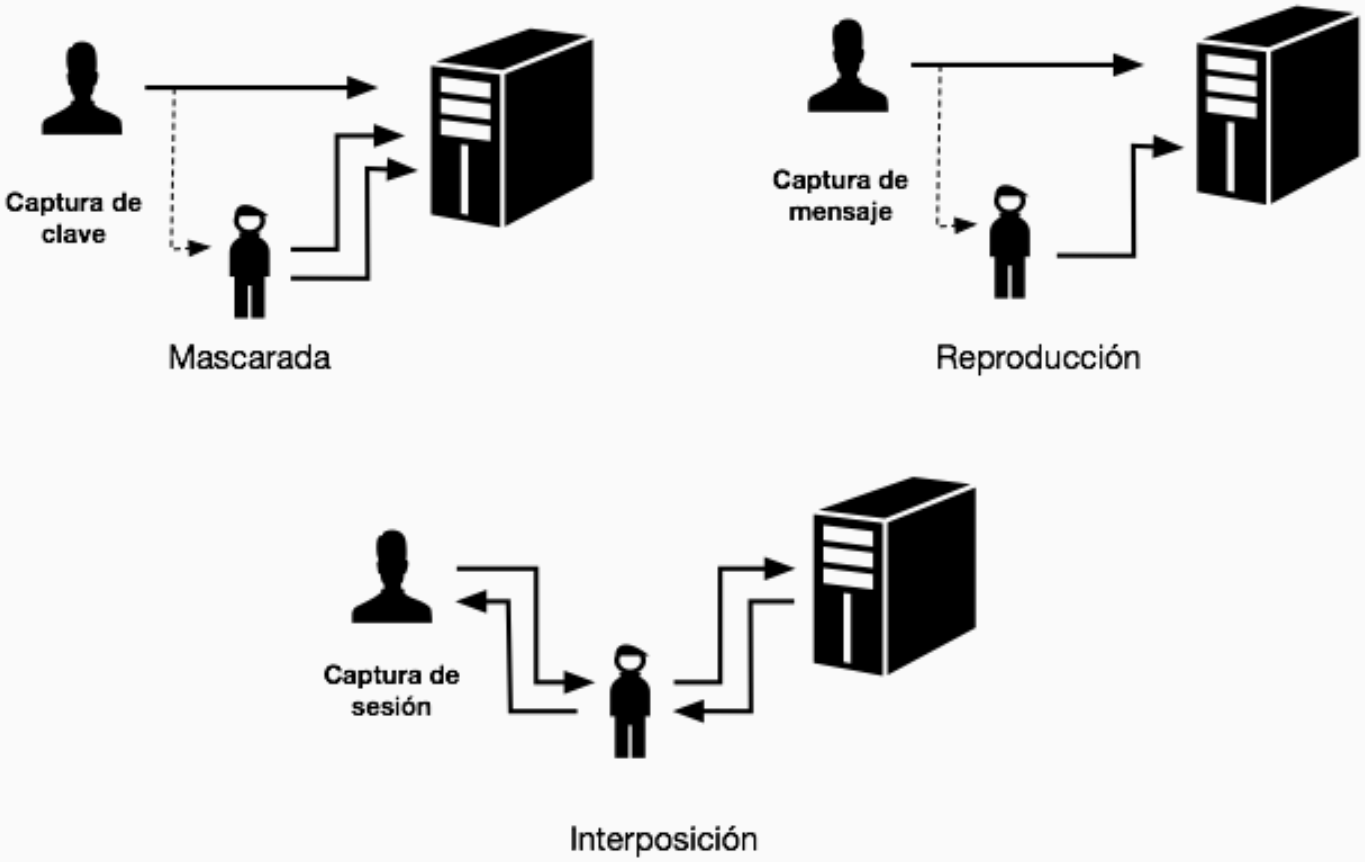

Figure 2:

Mascarada

En éste un participante en una comunicación pretende ser otra persona (o equipo). Mediante este mecanismo, los atacantes rompen la autenticación, es decir, la corrección de la identificación; como consecuencia, pueden obtener tipos de accesos que normalmente no podrían disfrutar.

Reproducción

Este método consiste en reproducir un intercambio de datos previamente capturado. Se produce así una repetición maliciosa o fraudulenta de una transmisión de datos válida. En ocasiones, esa reproducción constituye el propio ataque, como por ejemplo cuando se repite una solicitud para transferir dinero, pero con el mensaje modificado.

Interposición

En este tipo de ataque un atacante se introduce dentro del flujo de datos de una comunicación, haciéndose pasar por el emisor a ojos del receptor y viceversa.

- En una comunicación en red, un ataque por interposición puede estar precedido por un secuestro de sesión (hijacking) en el que se intercepta una sesión de comunicación activa.

Niveles de seguridad

Para proteger un sistema, se deben adoptar las necesarias medidas de seguridad en cuatro niveles distintos (que se describen más abajo): físico, humano, sistema operativo y red.

- Para garantizar la seguridad del sistema operativo, es necesario garantiza la seguridad en los primeros dos niveles.
- Cualquier debilidad en uno de los niveles altos de seguridad (físico o humando) permitirá puentear las medidas de seguridad que son estrictamente de bajo nivel (sistema operativo o red).

Niveles de seguridad

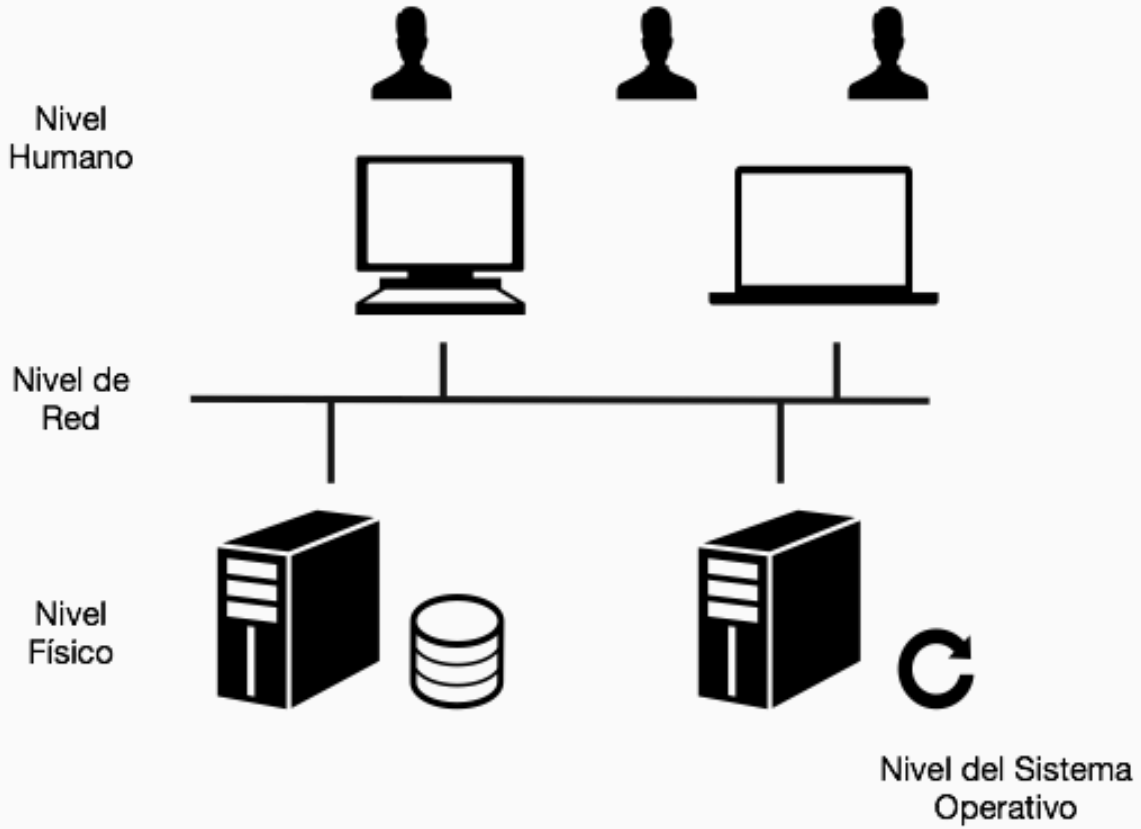

Figure 3:

Físico

Hay que dotar de seguridad tanto a las habitaciones donde las máquina residen como a los terminales o estaciones de trabajo que tengan acceso a dichas máquinas.

Humano

La autorización de los usuarios debe llevarse a cabo con cuidado, para garantizar que sólo los usuarios apropiados tengan acceso al sistema.

Sin embargo, los usuarios pueden ser engañados, para permitir el acceso a otros, utilizando técnicas de ingeniería social tales como:

- phising: un correo electrónico o página web de aspecto auténtico indican al usuario que brinde información confidencial.
- análisis de desperdicios: recopilar información para obtener acceso no autorizado a partir de archivos borrados, o papeles. [Silbertschaz,pp.512]

Sistema Operativo

El sistema debe autoprotergerse frente a posibles fallos de seguridad accidentales o premeditados.

Red

La interceptación de datos en la red puede ser tan dañina como el acceso al computador, y la interrupción de la comunicación podría constituir una ataque remoto de denegación de servicio.

Amenazas de programas (desde el exterior)

A continuación se describen algunos métodos comunes mediante los que los programas pueden provocar brechas de seguridad.

Amenazas de programas (desde el exterior)

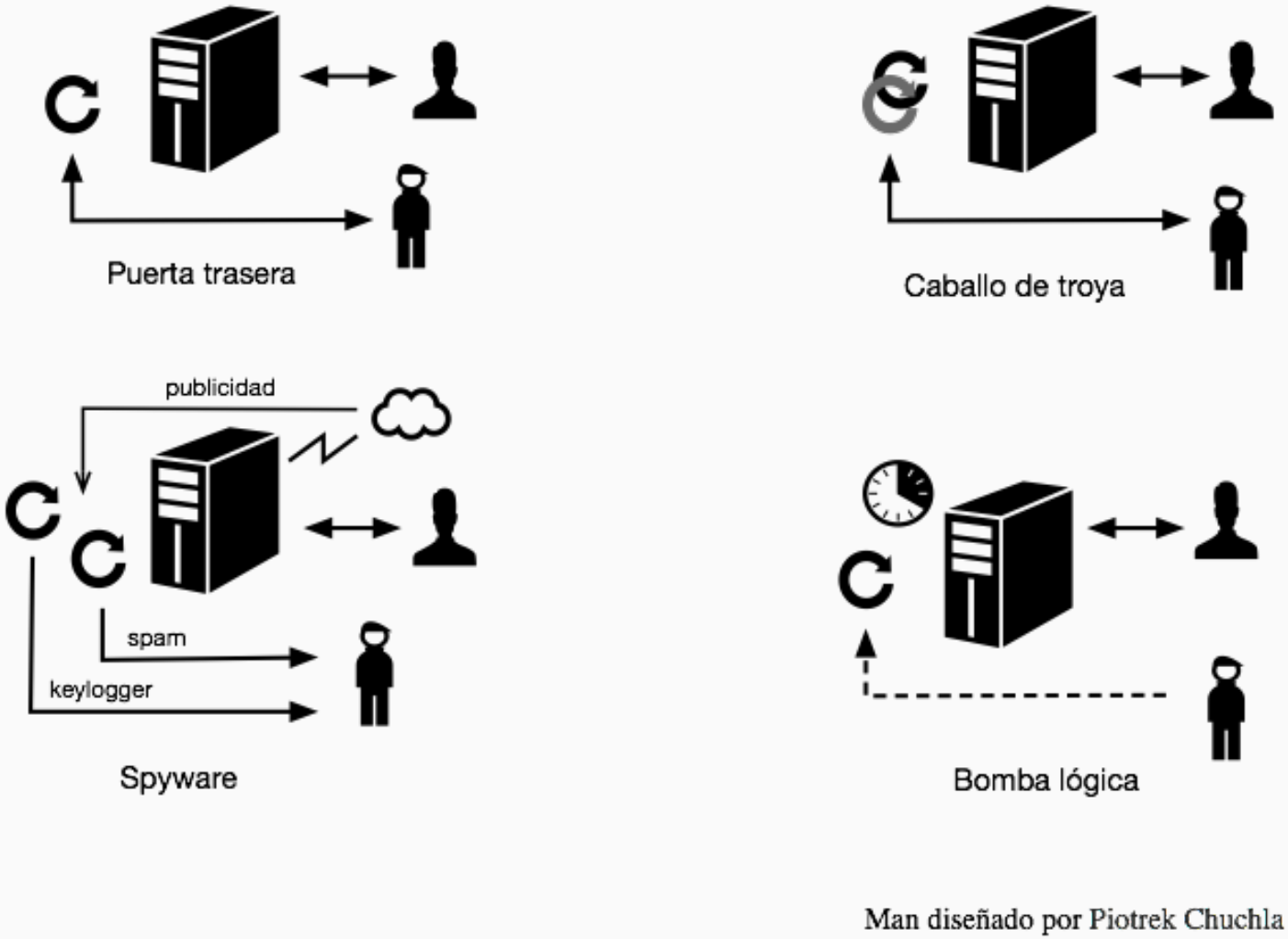

Figure 4:

Caballo de Troya

Existen programas escritos por unos usuarios que pueden ser ejecutados por otros.

- Si estos programas se ejecutan en un dominio que proporcione los derechos de acceso del usuario ejecutante, los otros usuarios podrían utilizar inapropiadamente estos derechos.
- Un segmento de código que utilice inapropiadamente su entorno se denomina caballo de Troya.

Caballo de Troya

Una variante del caballo de Troya es un programa que emula el típico programa de inicio de sesión (suplantación de identidad en el inicio de sesión).

- Un usuario que no esté advertido y ejecute dicho programa falso tratará de iniciar la sesión y observará que aparentemente ha escrito mal su contraseña, después, vuelve a intentarlo y esta vez lo hace con éxito.

Caballo de Troya

La única manera real de evitar esto es hacer que la secuencia de inicio de sesión empiece con una combinación de teclas que el programa falso no pueda detectar.

- Windows utiliza Ctr-Alt-Del con este fin.

Caballo de Troya

Otra variante es el spyware. El objetivo del spyware es descargar anuncios para mostrarlos en el sistema del usuario, crear ventanas de explorador emergentes cuando se visiten ciertos sitios o capturar información del sistema del usuario y enviarla a un sitio central.

Puerta trasera (trampa)

El diseñador de un programa o un sistema puede dejar detrás suyo un agujero en el software que sólo él sea capaz de utilizar.

- Este tipo de brecha de seguridad se conoce como puerta trasera.
- Por ejemplo, el código puede tratar de detectar un ID de usuario o una contraseña específicos y, al detectarlo, evitar los procedimientos de seguridad normales.

Puerta trasera (trampa)

Las puertas traseras plantean un difícil problema porque, para detectarlas, se debe analizar todo el código fuente de todos los componentes del sistema.

- En grandes sistemas, este análisis no se lleva a cabo frecuentemente.

Bomba lógica

Este mecanismo consiste en una pieza de código escrita generalmente por uno de los programadores de una empresa (que en ese momento es empleado), y se inserta de manera secreta en el sistema en producción.

Bomba lógica

El código verificaría si el empleado todavía continúa contratado por la empresa; en caso de no ser así, se activaría la bomba.

- Al activarse la bomba tal vez empiece a borrar archivos al azar, realizando pequeños cambios en los programas principales del sistema, o algún otro tipo de daño en la instalación.

Desbordamiento de pila

Lo que hace el atacante es aprovechar un error de un programa.

- El error puede deberse a un simple descuido del programador, en que éste se olvidó de comprobar el límite para un determinado parámetro de entrada.

Desbordamiento de pila

En este caso el atacante envía más datos de los que espera el programa.

- Utilizando prueba y error, o examinado el código fuente del programa, el atacante determina la vulnerabilidad y escribe un programa para aprovechar este hueco en la seguridad.

Desbordamiento de pila

Los pasos que ejecuta el atacante son:

- Desbordar un parámetro de entrada, un argumento de línea de comandos o un búfer de entrada hasta escribir en la zona correspondiente a la pila.
- Sobreescribir la dirección actual de retorno de la pila, sustituyéndola por la dirección del código de ataque.
- Escribir un fragmento simple de código en el siguiente espacio de la pila, que incluye los comandos que el atacante quiera ejecutar, por ejemplo arrancar un programa shell.

El resultado de la ejecución de este programa será un shell root o la ejecución de otro comando privilegiado.

Desbordamiento de pila

Una solución a este problema es que la CPU disponga de una característica que no permita la ejecución de código contenido en la sección de pila de la memoria.

- Esta implementación implica el uso de un nuevo bit dentro de las tablas de página de la CPU.
- Este bit marca la página asociada como no ejecutable, impidiendo leer y ejecutar instrucciones desde ella.

Virus

Los virus son programas que se pueden reproducir a sí mismos al adjuntar su código a otro programa legítimo, ellos están diseñados para infectar otros programas y equipos.

- Pueden causar estragos en un sistema modificando o destruyendo archivos y provocando funcionamiento inadecuado de los programas y fallos catastróficos en el sistema.

Virus

Algunos tipos de virus son muy dependientes de la arquitectura, sistema operativo y aplicaciones para las que fueron creados. Normalmente se propagan mediante correos electrónicos, o descarga de archivos infectados.

Virus

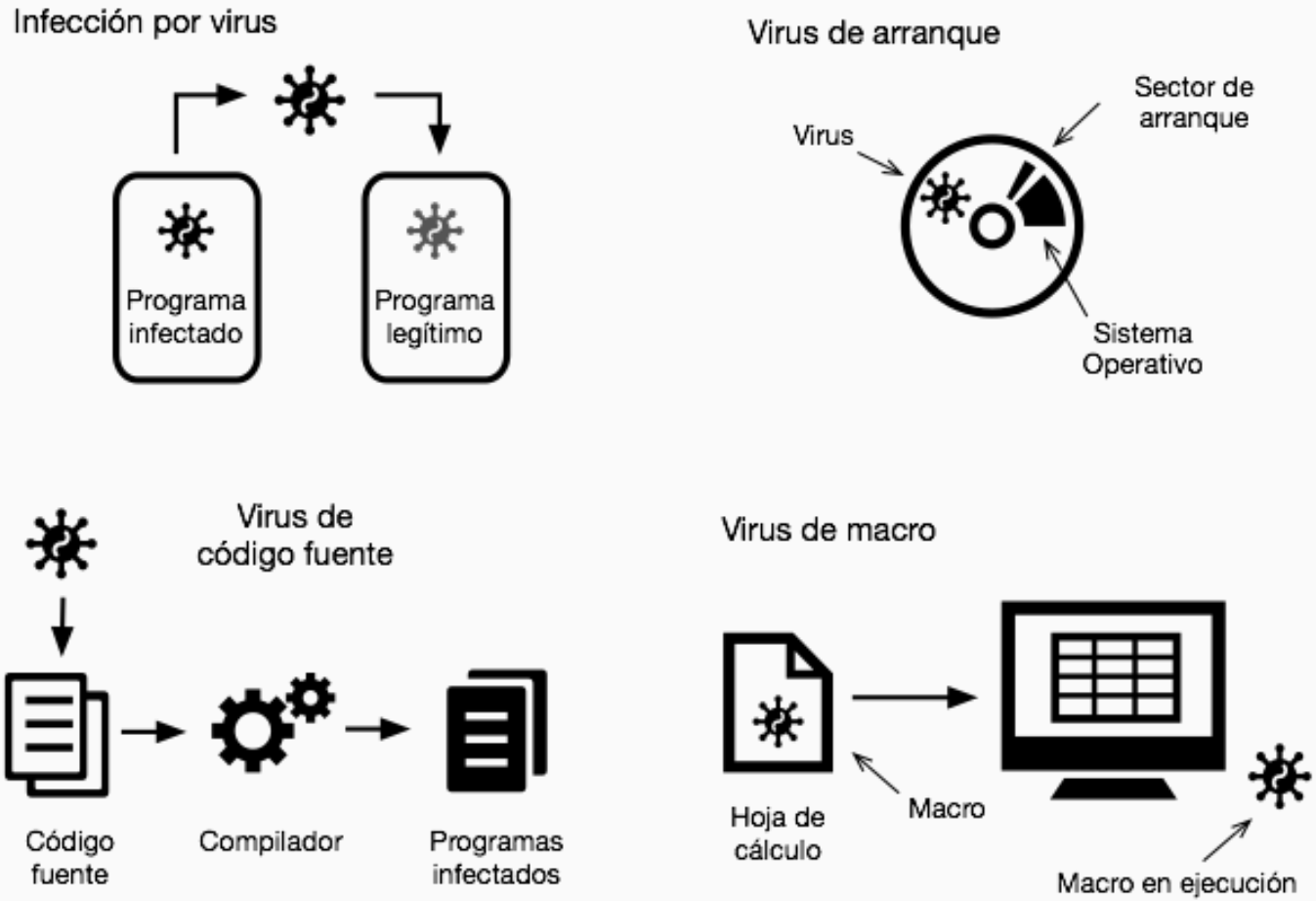

Figure 5:

Virus

Los virus se pueden clasificar en varias categorías generales, sin embargo, un mismo virus se puede pertenecer a más de una categoría a la vez:

Archivo o ejecutable

Este virus (también llamado parásito) infecta un sistema insertándose a un archivo y modificando el inicio del programa para que la ejecución salte al código del virus.

- Después de ejecutarse, el virus devuelve el control al programa para que no pueda detectarse que el virus se ha ejecutado.

Archivo o ejecutable

El virus se puede adjuntar al inicio del programa ejecutable, lo cuál es difícil pues se debe relocalizar el código del programa legítimo; al final del programa ejecutable, lo que hace que el virus deba poderse ejecutar independiente de su posición; o entre los espacios libres de cada segmento del programa ejecutable.

- Este último método, conocido como virus de cavidad, brinda la ventaja adicional de que el tamaño del archivo ejecutable no cambia.

Arranque

Este tipo de virus (también llamado virus de memoria) infecta el sector de arranque del sistema, ejecutándose cada vez que el sistema se arranca y antes que se cargue el sistema operativo.

- El virus busca luego otros medios de arranque (memorias usb) y también los infecta.
- El virus se almacena oculto en sectores del disco que marca como defectuosos.
- Al cargarse se oculta en la parte superior de la memoria, o en una entrada del vector de interrupciones que no se utilice.
- En el momento del arranque la máquina se encuentra en modo kernel y los antivirus no han empezado a ejecutarse, por lo que el virus puede realizar cualquier acción que desee.

Arranque

Generalmente este tipo de virus se oculta como un manejador de dispositivo que se activa cada vez que se ejecuta la interrupción asociada, pues antes ha alterado el vector de interrupciones.

- De esta forma cada vez que se ejecute la interrupción del dispositivo original el virus obtendrá nuevamente el control.

Macro

Estos virus están escrito en lenguajes de macros como Visual Basic.

- Estos virus se activan cuando se inicia un programa capaz de ejecutar la macro, por ejemplo en procesadores de palabras y hojas de cálculo.

Macro

Una forma de evitar este problema es que la aplicación le solicite al usuario si desea ejecutar las macros del documento, sin embargo, muchos usuarios no entienden lo que esto significa y lo permiten sin conocer sus consecuencias.

- Además, muchos documentos contienen macros legítimas que podrían ser ignoradas por la aplicación y volver inutilizables dichos documentos.

Macro

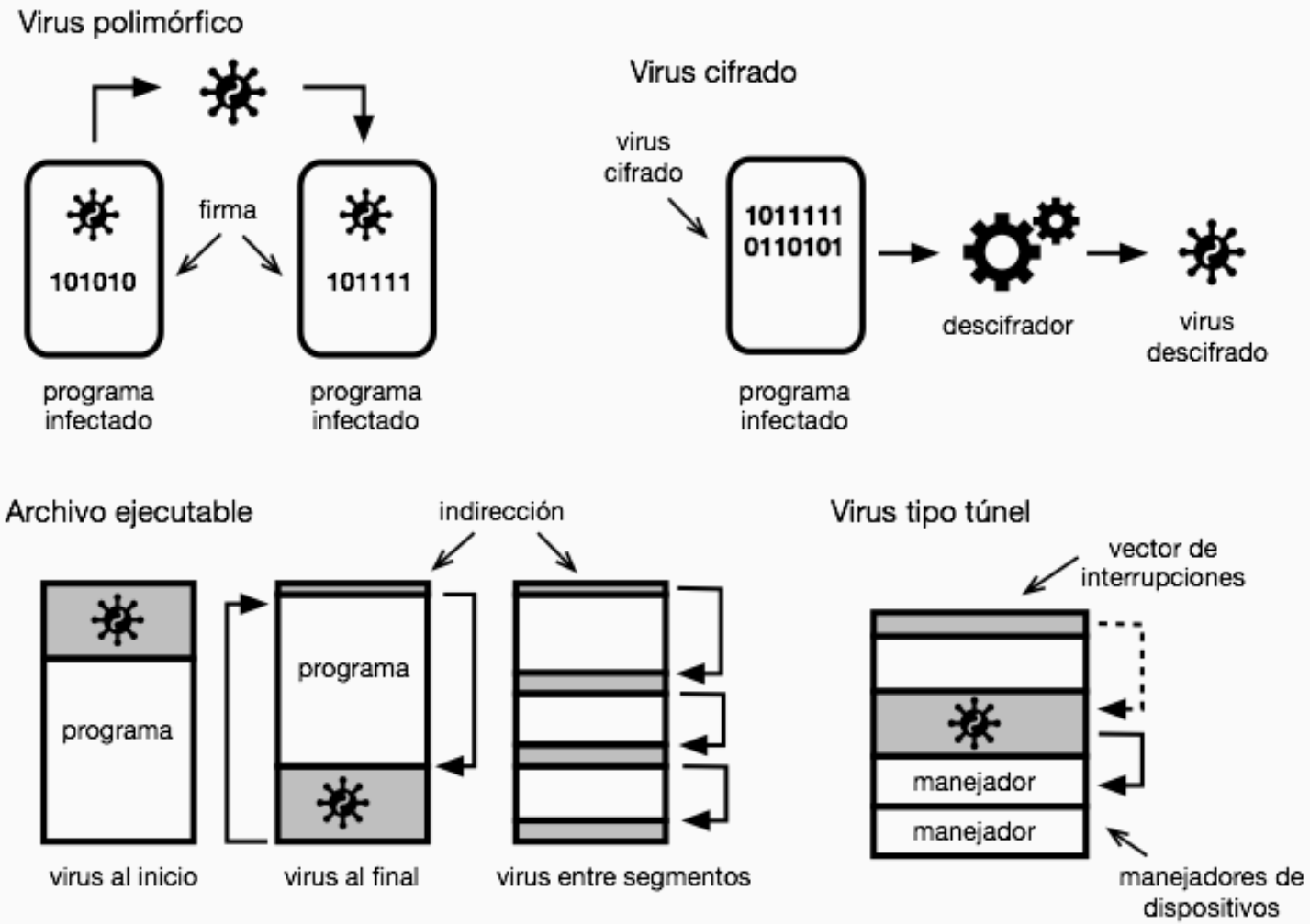

Figure 6:

Código fuente

Un virus de código fuente busca código fuente y lo modifica para incluir el virus y ayudar a su distribución.

- Las instrucciones que llaman al virus se deben colocar en un lugar adecuado del programa fuente, por ejemplo al final del "main" o antes de una instrucción "return" de un programa C.
- En el momento que el código sea compilado el virus quedará incrustado en el programa ejecutable.

Código fuente

Este es uno de los tipos de virus más portátiles, que significa que no son dependientes de la arquitectura o sistema operativo que se utilice.

- Más aún, la proliferación de aplicaciones escritas en lenguajes interpretados tales como PHP, Javascript o Python hacen que cada día sea más probable la aparición de este tipo de virus.

Polimórfico

Este tipo de virus cambia cada vez que se instala, para evitar su detección por parte del software antivirus.

- Los cambios no afectan a la funcionalidad del virus, sino que sólo modifican la signatura (firma) del virus.
- La signatura es un patrón que puede usarse para identificar un virus, generalmente una serie de bytes que forman parte del código del virus.

Cifrado

Un virus cifrado incluye código de descripción junto con el virus cifrado, de nueva para evitar la detección.

- El virus se descifra primero y luego se ejecuta.

Encubierto (rootkits)

Estos virus tratan de evitar la detección modificando partes del sistema que podrían ser usadas para detectarlos, por ejemplo la llamada al sistema read.

Túnel

Este tipo de virus trata de evitar la detección instalándose en la cadena de rutinas de tratamiento de interrupciones.

- Otros virus similares se instalan en los controladores de dispositivos.

Multiparte

Estos virus son capaces de infectar múltiples partes de un sistema, incluyendo los sectores de arranque, la memoria y los archivos.

- Por lo que son difíciles de detectar y evitar su propagación.

Acorazado

Este tipo de virus están codificados de tal manera que resulten difíciles de desentrañar y de comprender por parte de los investigadores que desarrollan los antivirus.

Amenazas del sistema y de la red

Las amenazas basadas en programas utilizan típicamente un fallo en los mecanismos de protección de un sistema para atacar a los programas.

- Por contraste, las amenazas del sistema y de la red implican el abuso de los servicios y de la conexiones de red.
- Las amenazas del sistema y de la red crean una situación en la que se utilizan inapropiadamente los recursos del sistema operativo y los archivos del usuario.
- Algunas de estas amenazas son: gusanos, el escaneo de puertos, y los ataques por denegación de servicio

Amenazas del sistema y de la red

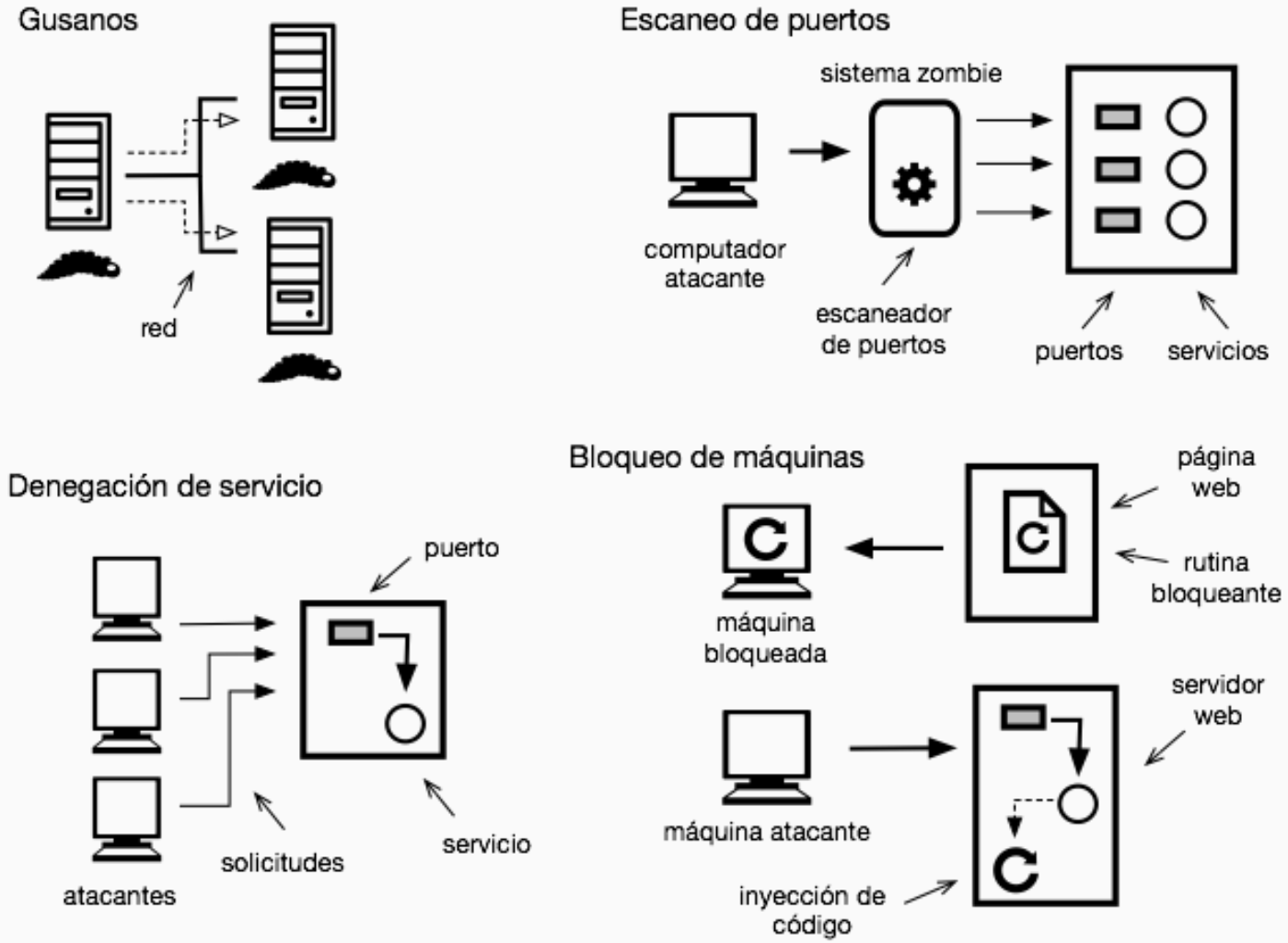

Figure 7:

Gusanos

Un gusano es un proceso que utiliza un mecanismo de reproducción para afectar el rendimiento del sistema.

- El gusano crea copias de sí mismo, utilizando recursos del sistema y en ocasiones impidiendo operar a todos los demás procesos.
- En las redes informáticas, los gusanos son particularmente potentes, ya que pueden reproducirse de un sistema a otro y colapsar una red completa.

Escaneo de puertos

El escaneo de puertos no es un ataque, sino más bien un método para que los piratas informáticos detecten las vulnerabilidades del sistema que puedan ser atacadas.

- El escaneo de puertos se realiza normalmente de forma automatizada, lo que implica utilizar una herramienta que trate de crear una conexión TCP/IP a un puerto o rango de puertos específicos.
- Para cada servicio que responda, un pirata podría intentar de utilizar un error conocido del servicio.
- Frecuentemente, estos errores son desbordamientos de búfer, que permiten la creación de un shell de comandos privilegiado.

Escaneo de puertos

Puesto que los escaneos de puertos son detectables, se suelen realizar desde sistemas zombi.

- Dichos sistemas son máquinas independientes y previamente comprometidas que están prestando servicio normal a sus propietarios al mismo tiempo que son utilizadas inadvertidamente para propósitos indebidos, incluyendo la realización de ataques por denegación de servicio y la retransmisión de correo basura.

Denegación de servicio

Los ataques de denegación de servicio se realizan generalmente a través de la red. Se los puede clasificar en dos categorías.

- El primer caso es el de los ataques que consumen tantos recursos de la máquina atacada que prácticamente no puede realizarse con ella ningún trabajo útil.
- Esto puede ser, por ejemplo, los recursos de la máquina cliente (bloqueo del cliente) mediante un script (javascript, java o flash) que se descarga en una página web; o bien, en el servidor (bloqueo del servidor) mediante la inyección de código (PHP, SQL, etc) desde un cliente.

Denegación de servicio

El segundo caso de ataque (bloqueo de la red) implica hacer caer la red o la instalación.

- Este tipo de ataque es el resultado de un abuso de alguna función fundamental del TCP/IP.
- Un ejemplo, es generar una gran cantidad de solicitudes de conexión TCP/IP pero no completarlas.

Denegación de servicio

Generalmente, es imposible prevenir los ataques de denegación de servicio.

- Los ataques utilizan los mismos mecanismos de la operación normal.
- Todavía más difíciles de prevenir y de solucionar son los ataques distribuidos de denegación de servicio (DDOS).
- Estos ataques se inician desde múltiples sitios a la vez, dirigidos hacia un objetivo común, normalmente por parte de programas zombis.

Criptografía

La criptografía se utiliza para restringir los emisores y/o receptores de una mensaje.

- La criptografía moderna se basa en una serie de secretos, denominados claves, que se distribuyen selectivamente a las computadoras de una red y se utilizan para procesar mensajes.

Criptografía

La criptografía permite al receptor de un mensaje verificar que el mensaje ha sido creado por alguna computadora que posee una cierta clave: esa clave es el origen del mensaje.

- De forma similar, un emisor puede codificar su mensaje de modo que sólo una computadora que disponga de una cierta clave pueda decodificar el mensaje, de manera que esta clave se convierte en el destino.
- Las claves están diseñadas de modo que no sea computacionalmente factible calcularlas a partir de los mensajes que se hayan generado con ellas, ni a partir de ninguna información pública.

Criptografía

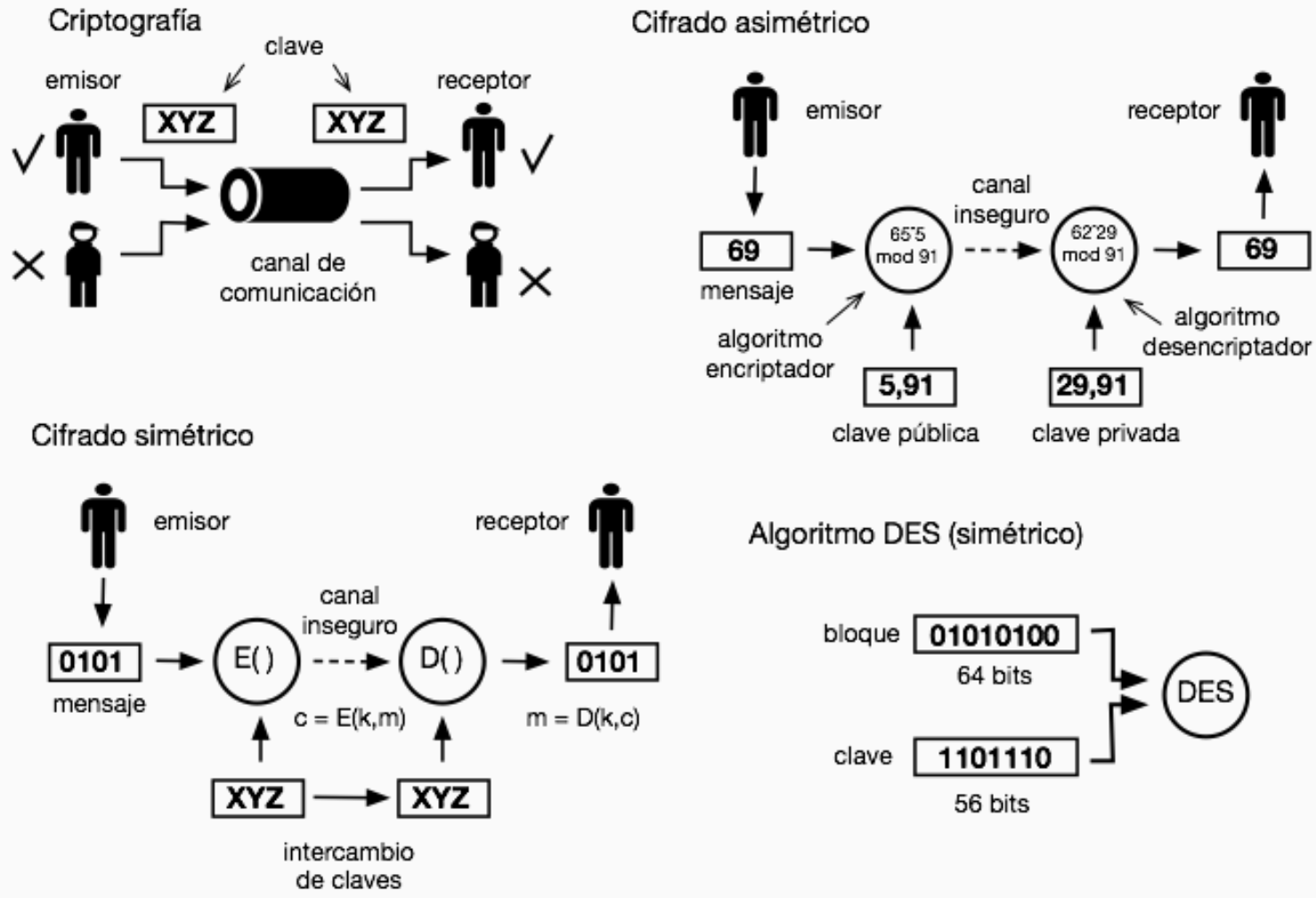

Figure 8:

Cifrado

El intercambio de claves puede tener lugar directamente entre las dos partes o través de una tercera parte de confianza (es decir, una autoridad de certificación).

Un algoritmo de cifrado consta de los siguientes componentes:

- Un conjunto K de claves
- Un conjunto M de mensajes
- Un conjunto C de mensajes de texto cifrado
- Una función E: K -> (M -> C) para generar texto cifrado
- Una función D: K -> (C -> M) para descifrar texto codificado

Cifrado

Un algoritmo de cifrado debe proporcionar la propiedad que: dado un mensaje de texto cifrado c en C, una computadora puede calcular m tal que E(k)(m)=c sólo si posee D(k).

Existen dos tipos principales de algoritmos de cifrado:

- simétricos y
- asimétricos.

Cifrado simétrico

El algoritmo de cifrado simétrico utiliza la misma clave para cifrar y para descifrar, es decir E(k) puede deducirse a partir de D(k) y viceversa.

- Por tanto, es necesario proteger el secreto de E(k) con el mismo grado que el de D(k).

Cifrado simétrico

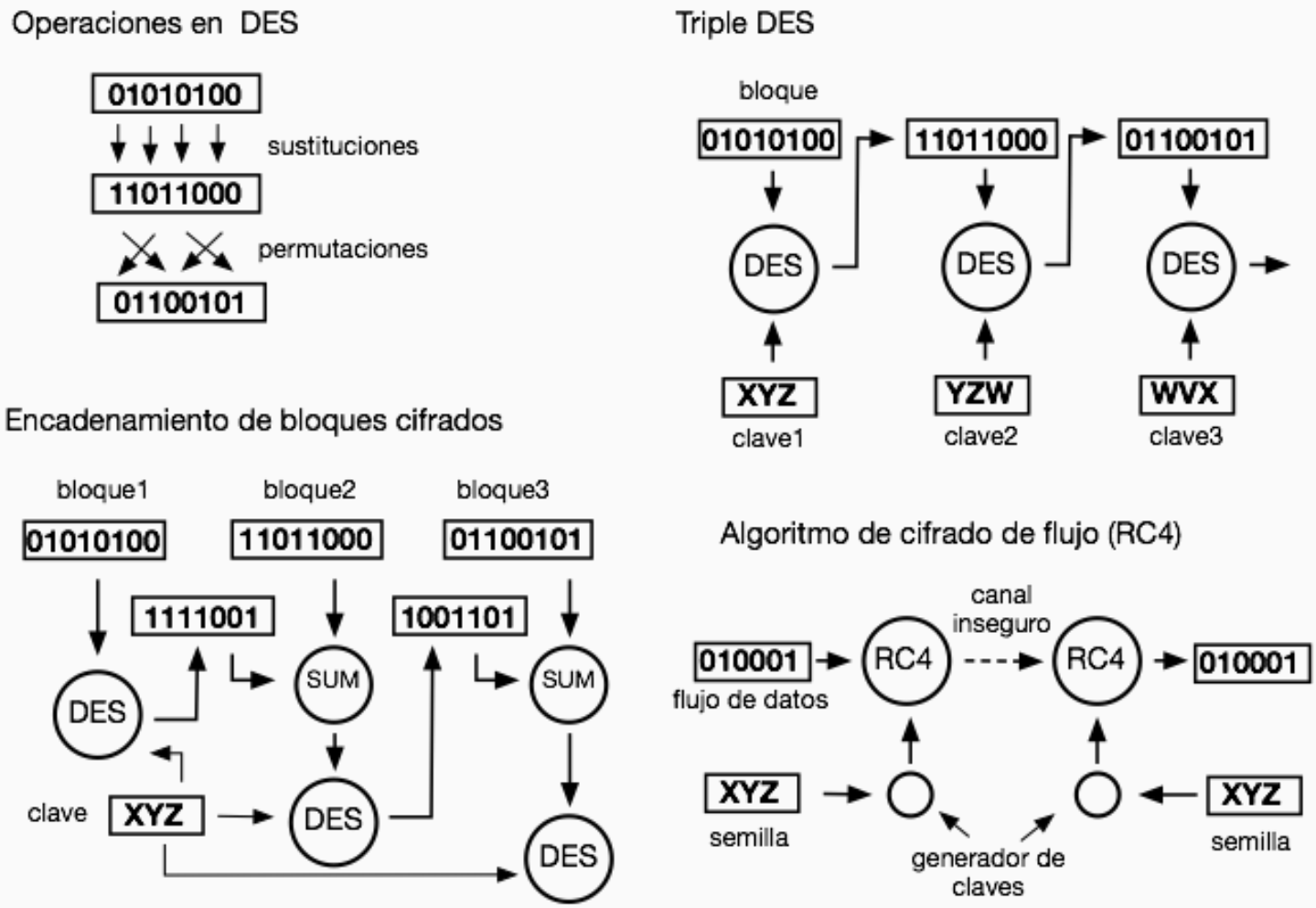

Figure 9:

Cifrado simétrico

El estándar DES funciona tomando un valor de 64 bits y una clave de 56 y realizando una serie de transformaciones.

- Estas transformaciones están basadas en operaciones de sustitución y permutación.
- Puesto que DES opera sobre un conjunto de bits simultáneamente, se denomina algoritmo de cifrado de bloque.

Una forma de mejorar este mecanismo es aplicar ¨encadenamiento de bloques cifrados¨ que consiste en realizar una operación XOR con el bloque de texto cifrado anterior antes de proceder al cifrado del texto actual.

Cifrado simétrico

Hoy en día existe una versión mejorada de DES, conocida como triple DES, en la que el algoritmo DES se repite tres veces sobre un mismo texto, utilizando dos o tres claves.

- Otros algoritmos de cifrado simétrico son: AES, twofish y RC5; los cuáles varían en cuanto al tamaño de la clave, el tamaño de bloque y el número de transformaciones que aplican.

Cifrado simétrico

RC4 es un algoritmo de cifrado de flujo el cual está diseñado para cifrar y descifrar un flujo de bytes o bits, en lugar de un bloque.

- La clave se introduce en un generador de bits pseudoaleatorio, que produce un flujo de claves.
- Un flujo de claves es un conjunto infinito de claves que pueden usarse para el flujo de texto que se proporciona como entrada.
- RC4 se utiliza para cifrar flujos en el protocolo de redes inalámbricas WEP y comunicaciones Web mediante SSL.

Cifrado asimétrico

En un algoritmo de cifrado simétrico, las claves de cifrado y descifrado son distintas.

- El algoritmo RSA de cifrado es un algoritmo de cifrado de bloque de clave pública y es el algoritmo asimétrico más ampliamente utilizado.

Cifrado asimétrico

El uso de un mecanismo de cifrado asimétrico comienza con la publicación de la clave pública del destino. Para la comunicación bidireccional, el origen debe también publicar su clave pública.

- Esa publicación puede ser tan simple como entregar una copia electrónica de la clave, o puede tratarse de un mecanismo más complejo.
- La criptografía asimétrica se basa en funciones matemáticas en lugar de en transformaciones, lo que hace que sea mucho más cara de implementar, en términos de recursos de computación requeridos.

Autenticación

El proceso de restringir el conjunto de potenciales emisores de un mensaje se denomina autenticación.

- La autenticación es, por tanto, complementaria al cifrado.
- Un mensaje cifrado también puede demostrar la identidad del emisor; por ejemplo si D(Kd,N)(E(ke,N)(m)) produce un mensaje válido, entonces se sabe que el creador del mensaje debe poseer ke.
- La autenticación también resulta útil para demostrar que un mensaje no ha sido modificado.

Autenticación

Un algoritmo de autenticación consta de los siguientes componentes:

- Un conjunto K de claves
- Un conjunto M de mensajes
- Un conjunto A de autenticadores
- Una función S:K -> (M -> A). Es decir, para cada k que pertenece a K, S(k) es una función para generar autenticadores a partir de mensajes. Tanto S como S(k) para cualquier k deben ser funciones computacionalmente eficientes.
- Una función V: K -> (MxA -> {true,false}). Es decir, para cada k pertenece a K, V(k) es una función para verificar autenticadores de mensajes. Tanto V coo V(k) para cualquier k deben ser funciones eficientemente computables.

Distribución de claves

Con los algoritmos simétricos, ambas partes necesitan la clave y ninguna otra persona debe disponer de ella.

- La tarea de suministrar la clave simétrica a sus usuarios legítimos constituye un reto importante.
- En ocasiones, esa distribución se hace fuera de banda, por ejemplo mediante un documento escrito o una conversación.

Autenticación de usuario

El sistema de protección depende de la capacidad de identificar los programas y procesos que están actualmente en ejecución, lo que a su vez depende de la capacidad de identificar a cada usuario del sistema. Normalmente, cada usuario se identifica a sí mismo.

Generalmente, la autenticación de usuario se basa en una o más de tres cuestiones:

- la posesión de algo (una clave o tarjeta) por parte del usuario
- el conocimiento de algo (un identificador de usuario y una contraseña) por parte del usuario
- un atributo del usuario (huella digital, patrón retinal o firma)

Autenticación de usuario

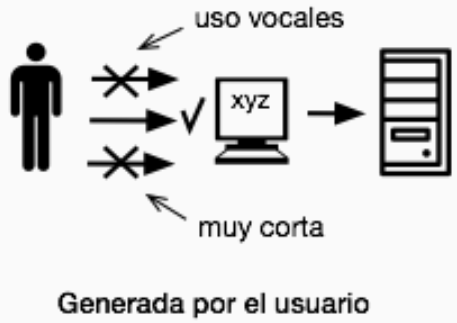

Figure 10:

Contraseñas

El método más habitual para autenticar la identidad de un usuario consiste en usar contraseñas.

- Cuando el usuario se identifica a sí mismo mediante un ID de usuario o un nombre de cuenta, se le pide una contraseña.
- Si la contraseña suministrada coincide con la contraseña almacenada en el sistema, se supone que el propietario está accediendo a la misma.

Vulnerabilidades de las contraseñas

Las contraseñas son comunes porque son fáciles de comprender y utilizar.

- Sin embargo, a menudo son fáciles de adivinar, ser mostradas por accidente, ser interceptadas o ilegalmente transferidas.

Vulnerabilidades de las contraseñas

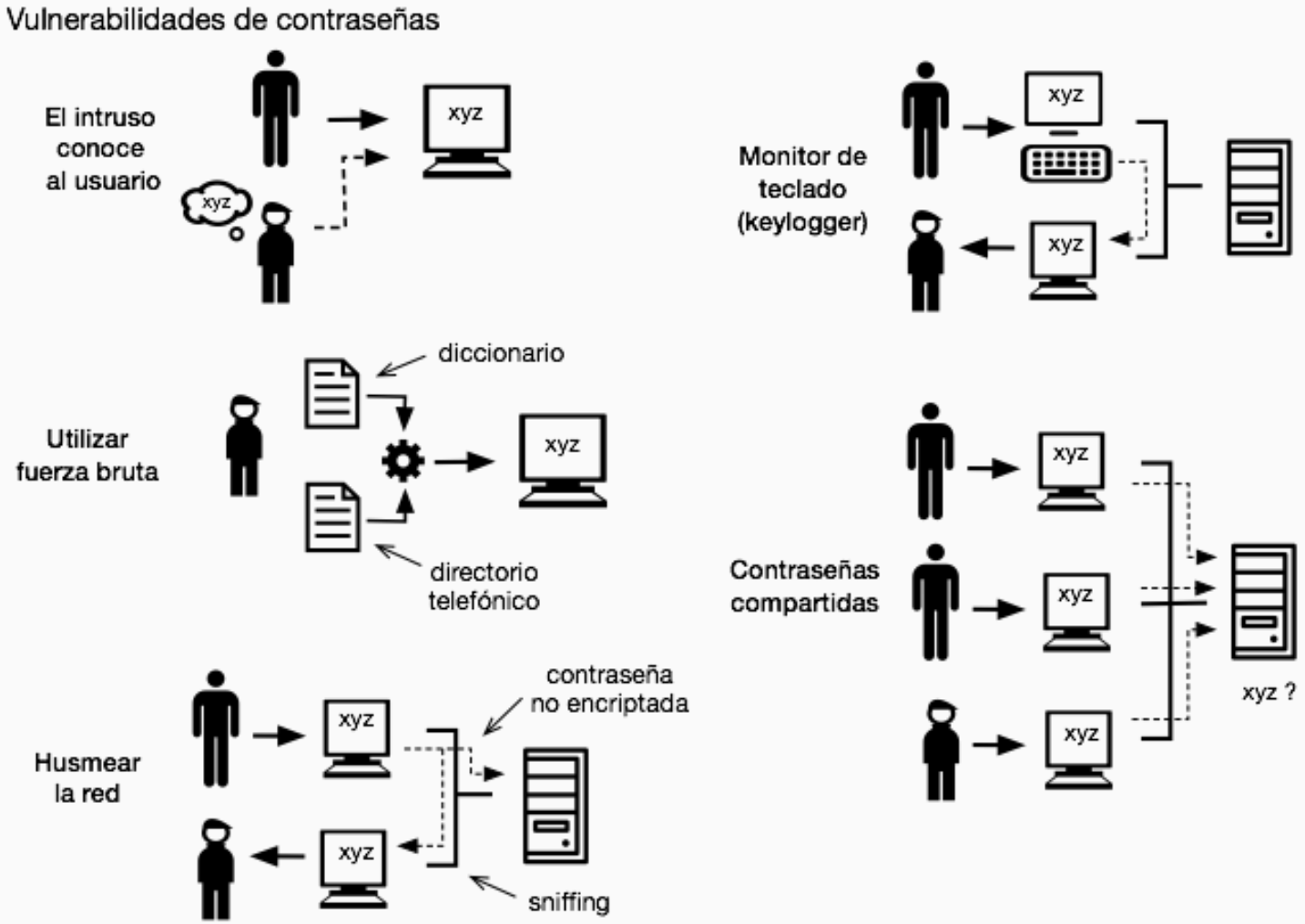

Figure 11:

Vulnerabilidades de las contraseñas

Existen dos formas de adivinar contraseñas:

- El intruso conoce al usuario o tiene información de él. Probablemente el usuario utiliza datos que le sean conocidos como contraseña.
- Utilizar la fuerza bruta, probando todas las posibles combinaciones. La gran mayoría de la gente utilizada contraseñas fáciles de adivinar.

Vulnerabilidades de las contraseñas

Las contraseñas también se pueden averiguar mediante mecanismos de monitorización visual o electrónica.

- Cualquiera con acceso a la red podría añadir un monitor de red y husmear (sniffing) los datos transferidos, incluyendo el ID de usuario y la contraseña. Lo anterior se resuelve cifrando el flujo de datos en la red.
- Otras forma de robar la contraseña es mediante un caballo de Troya en el sistema, que capture las pulsaciones de tecla (key logger) antes de ser enviadas a la aplicación.

Vulnerabilidades de las contraseñas

Otro tipo de amenaza es la trasferencia ilegal de las contraseñas por parte de los mismos usuarios.

- En algunas instalaciones los usuarios comparten contraseñas para acceder a algún tipo de servicio.
- Si se produce una intrusión no autorizada es difícil saber quién es el responsable.

Vulnerabilidades de las contraseñas

Las contraseñas pueden ser generadas por el sistema o seleccionadas por el usuario.

- Si son generadas por el sistema normalmente son difíciles de memorizar y el usuario las anotará en algún lado, lo que puede ocasionar que sea sustraída.
- Para evitar que el usuario seleccionen contraseñas sencillas se puede tener un mecanismo que obligue a elegir contraseñas con cierto grado de complejidad: no uso de vocales, letras que no se repitan, uso combinado de letras y números, uso alternado de mayúsculas y minúsculas y longitud mínima.
- Otra opción es obligar a cambiar la contraseña cada cierto período de tiempo.

Contraseñas cifradas

Algunos sistemas utilizan el cifrado para evitar la necesidad de mantener en secreto el archivo de contraseñas.

- Cada usuario tiene una contraseña.
- El sistema contiene una función que es muy difícil de invertir, pero fácil de calcular.
- Esta función se emplea para codificar todas las contraseñas y sólo se almacenan las contraseñas codificadas.

Contraseñas cifradas

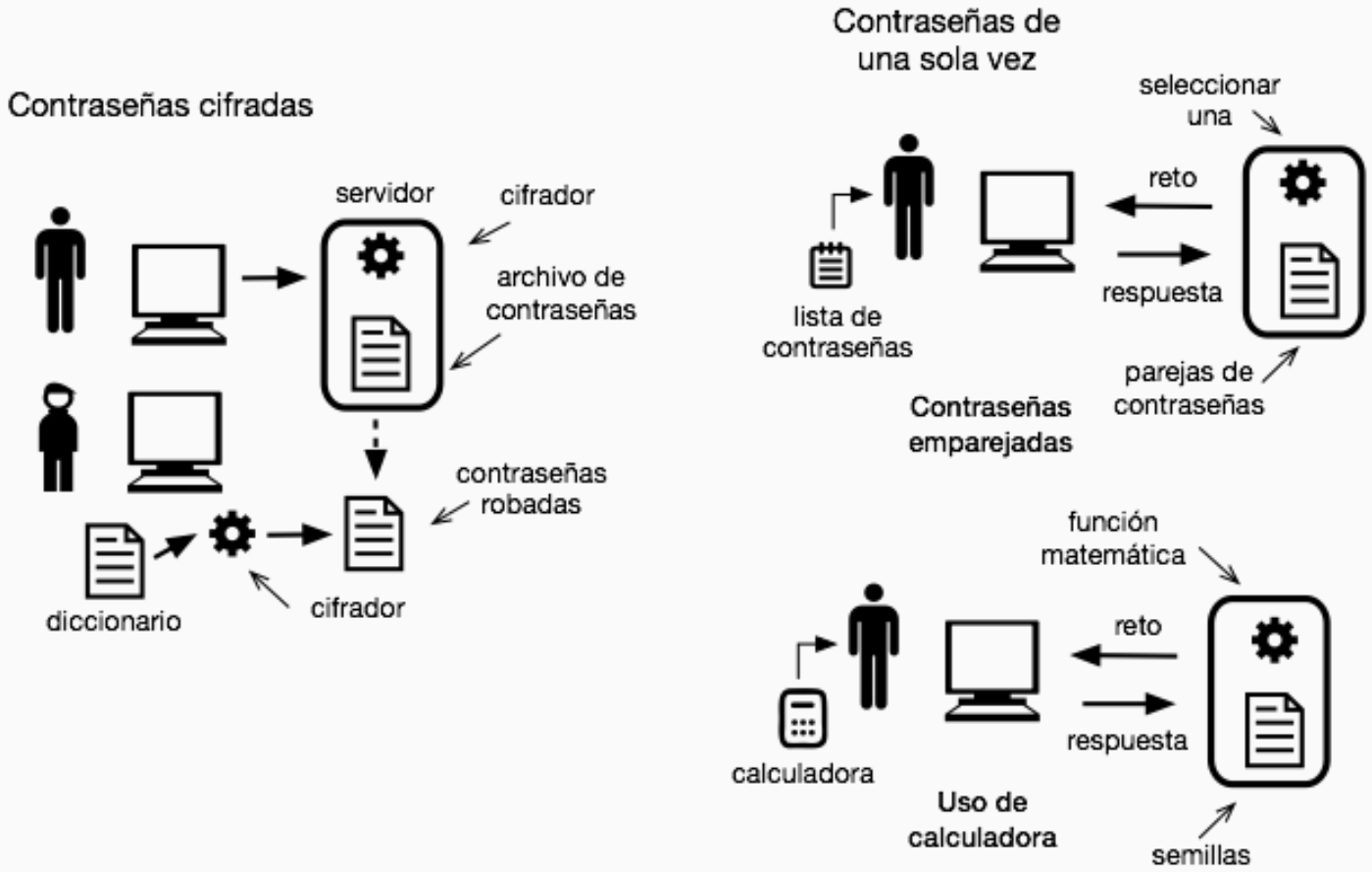

Figure 12:

Contraseñas cifradas

Cuando un usuario presenta una contraseña, se codifica y se compara con la contraseña codificada que se tiene almacenada.

- Aunque esta contraseña codificada pueda verse, no puede codificarse, por lo que no es posible determinar la contraseña real.
- Por tanto no es necesario mantener en secreto el archivo de contraseñas.

Contraseñas cifradas

Debido a que todos los usuarios podrían tener acceso a este archivo, sería fácil codificar combinaciones de palabras y compararlas con las contraseñas del archivo.

- De esta forma se podrían obtener las contraseñas sencillas de algunos otros usuarios del sistema.
- Una forma de evitar esto es que solo el superusuario tenga acceso a dicho archivo.
- Un método mejor es incluir un número aleatorio en la contraseña para asegurar que, si dos contraseñas son iguales sin cifrar, darán lugar a contraseñas cifradas diferentes.

Contraseñas de un solo uso

Un sistema podría usar un conjunto de contraseñas emparejadas.

- Cuando se inicia una sesión, el sistema seleccionar aleatoriamente una pareja de contraseñas y presenta una parte de la misma; el usuario debe suministrar la otra parte.
- En este sistema, el usuario es desafiado y debe responder con la respuesta correcta a dicho desafío.

Contraseñas de un solo uso

Este método se puede generalizar, utilizando un algoritmo como contraseña.

- Por ejemplo, el algoritmo puede ser un función entera: el sistema selecciona un entero aleatorio y lo presenta al usuario.
- El usuario aplica la función y responde con el resultado correcto.
- El sistema también aplica la función. Si los dos resultados corresponden, se permite el acceso.

Contraseñas de un solo uso

En este sistema de contraseña de un solo uso, la contraseña es diferente en cada caso.

- Cualquiera que capture la contraseña de una sesión e intente reutilizarla en otra sesión no tendrá éxito.
- Para implementar este mecanismo de seguridad existentes dispositivos hardware y de software, generalmente en forma de calculadora.
- Otra variante es utilizar un libros de códigos, que es una lista de contraseñas de un sólo uso. en este método, cada contraseña de la lista se usa, por orden, una vez y luego se tacha o se borra.

Utilizando objetos físicos

Otro método para autenticar usuarios es comprobar algún objeto físico que tengan, en lugar de algo que sepan.

- Generalmente se utiliza una tarjeta de plástico que se en un lector asociado con la computadora.
- Por lo general, el usuario también debe escribir una contraseña para evitar que alguien utilice una tarjeta perdida o robada.

Utilizando objetos físicos

Existen dos tipos de tarjetas de plástico:

- tarjetas de tira magnética y
- tarjetas de chip.

Utilizando objetos físicos

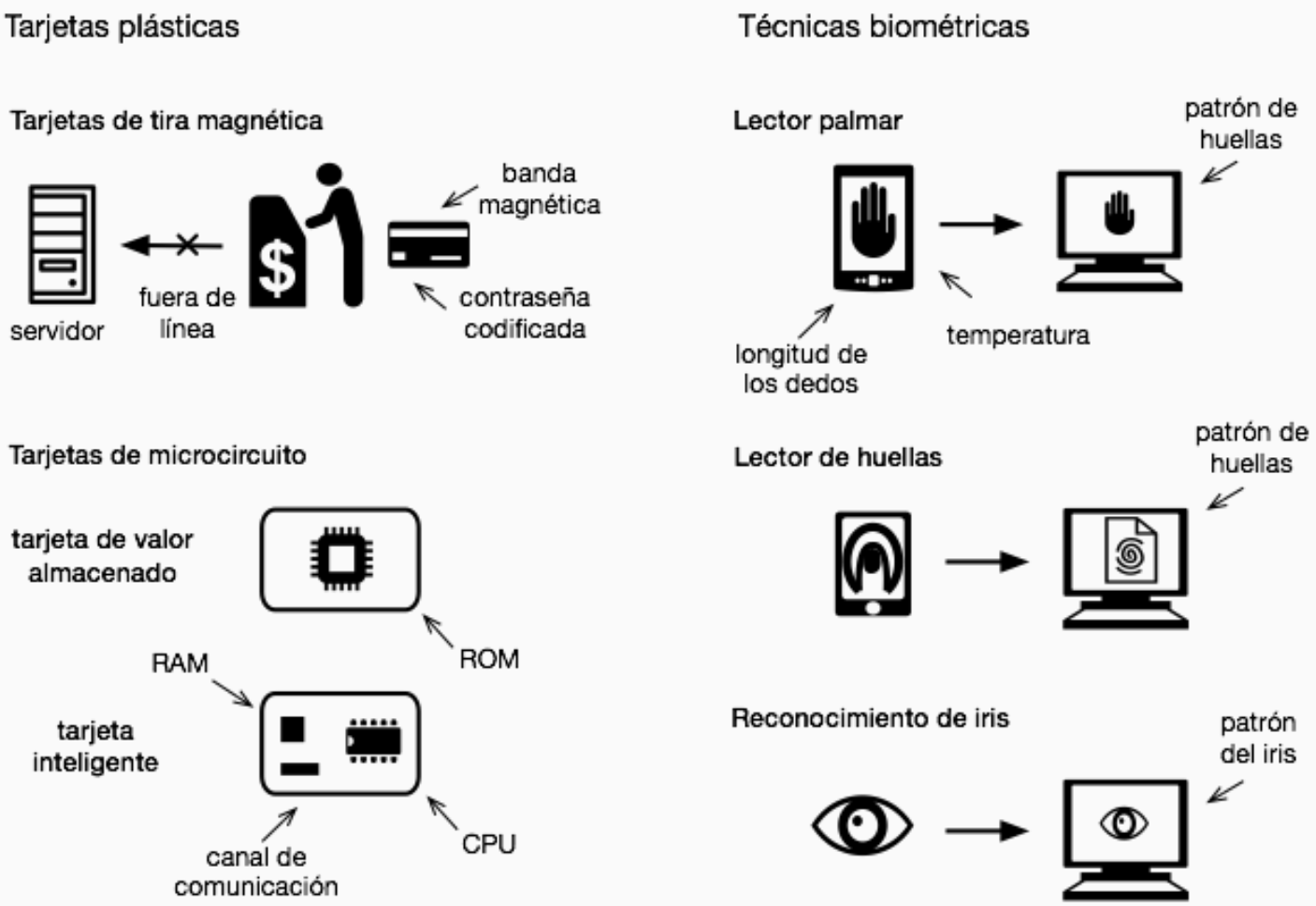

Figure 13:

Utilizando objetos físicos

Las tarjetas de tira magnética contienen información escrita en una pieza de cinta magnética pegada a la parte posterior de la tarjeta.

- Generalmente la tarjeta contiene la contraseña del usuario cifrada, de forma que una terminal "fuera de línea" puede verificar la autenticidad del usuario.
- Este tipo de tarjetas son riesgosas pues el equipo para leerlas y copiarlas es económico y está disponible en muchas partes.

Utilizando objetos físicos

Las tarjetas de chip contienen un pequeño chip. Estas tarjetas se pueden subdividir en dos categorías: tarjetas de valor almacenado y tarjetas inteligentes.

- Las tarjetas de valor almacenado contienen una pequeña cantidad de memoria que utiliza tecnología ROM pero no contienen un CPU.
- Las tarjetas inteligentes poseen un CPU, ROM, RAM y un canal de 9600 bps.

Utilizando objetos físicos

La gran ventaja de las tarjetas inteligentes es que no necesitan una conexión en línea con un banco, ellas mismas almacenan internamente y modifican los montos necesarios.

- Este tipo de tarjetas puede ser actualizada con nuevas versiones de software, p.ej., un algoritmo criptográfico.

Biométrica

Un lector palmar o de manos establece la correspondencia entre los parámetros almacenados y los que se obtienen mediante los lectores de manos.

- Los parámetros pueden incluir un mapa de temperaturas, así como la longitud del dedo, la anchura del mismo y los patrones de las líneas.
- Pero son demasiado grandes y caros para ser utilizados en computadoras normales.

Biométrica

Los lectores de huellas digitales son muy precisos y su relación coste-efectividad es buena.

- Estos dispositivos leen los patrones de las líneas del dedo y los convierten en una secuencia de números.
- El software puede entonces explorar un dedo situado sobre la almohadilla y comparar sus características con estas secuencias almacenadas, para determinar si el dedo es el mismo que tiene almacenado.
- El problema es que los usuarios asocian la toma de huellas con criminales.

Biométrica

Otro mecanismo es el reconocimiento de iris.

- No hay dos personas que tengan los mismos patrones de iris, por lo que el método es tan bueno como el de las huellas digitales y se automatiza con facilidad.
- Sin embargo, puede ser engañado presentando una fotografía de los ojos de otra persona.
- Para evitar esto, el mecanismo puede activar un flash y determinar si existe una contracción de la pupila.
- La autenticación mediante múltiples factores es todavía mejor, por ejemplo emplear un dispositivo USB, un PIN y un escáner de huella digital.

Implementación de defensas de seguridad

La mayor parte de los profesionales de la seguridad defienden la teoría de la defensa en profundidad, la cual establece que es mejor utilizar más niveles de defensa que menos.

Política de seguridad

La evaluación de la seguridad puede cubrir un amplio espectro, desde la ingeniería social a la evaluación de riesgos y los análisis de puertos.

- La actividad principal de la mayor parte de las evaluaciones de vulnerabilidad es una prueba de penetración, en la que se analiza la entidad para conocer las vulnerabilidades.

Política de seguridad

Un análisis de un sistema individual puede comprobar el siguiente conjunto de aspectos del sistema:

- Contraseñas cortas o fáciles de adivinar
- Programas privilegiados no autorizados
- Programas no autorizados en directorios del sistema
- Protecciones inapropiadas en los directorio del sistema

Evaluación de la vulnerabilidad

La detección de intrusiones, como su nombre sugiere consiste en detectar los intentos de intrusión y las intrusiones que hayan tenido éxito en los sistemas informáticos, e iniciar las apropiadas respuestas a dichas intrusiones.

Detección de intrusiones

La detección de intrusiones consiste en detectar los intentos de intrusión y las intrusiones que hayan tenido éxito en los sistemas informáticos, e iniciar las apropiadas respuestas a dichas intrusiones.

Detección de intrusiones

La detección de intrusiones conlleva una amplia matriz de técnicas, que varían según diversos ejes:

- El instante en que se produce la detección.
- Los tipos de informaciones examinadas para detectar la actividad de intrusión.
- El rango de las capacidades de respuesta: alertar a un administrador.

Protección frente a virus

A menudo se emplean programas antivirus para proporcionar esta protección.

- Algunos de estos programas son efectivos sólo frente a algunos virus concretos conocidos; estos programas funcionan buscando en todos los programas del sistema el patrón específico de instrucciones conocidas que definen el virus.
- Cuando encuentran un patrón conocido, eliminan las instrucciones, desinfectando el programa.
- Los programas antivirus pueden disponer de catálogos de miles de virus, que son los que tratan de buscar.

Protección frente a virus

Algunos programas antivirus también realizan un análisis integral en lugar de limitarse a analizar los archivos contenidos en el sistema de archivos: buscan en los sectores de arranque, en la memoria, en los correos electrónicos, en los archivos descargados, en los archivos almacenados en dispositivos extraíbles, etc.

Auditoría, contabilización y registro

La auditoría,la contabilización y la elaboración de registros pueden disminuir el rendimiento del sistema, pero resultan útiles en diversas áreas, incluyendo la de la seguridad.

- Pueden registrarse todas las ejecuciones de llamadas al sistema, para poder analizar el comportamiento del sistema, pero normalmente sólo se registran los sucesos sospechosos.

Cortafuegos para proteger los sistemas y redes

Un cortafuegos es una computadora, dispositivo o encaminador que se sitúa entre el sistema seguro y el que no lo es. Un cortafuegos de red limita el acceso a la red entre los dos dominios de seguridad y monitoriza y registra todas las conexiones.

- También puede limitar las conexiones basándose en la dirección de origen o de destino, el puerto de origen o de destino o la dirección de la conexión.

Cortafuegos para proteger los sistemas y redes

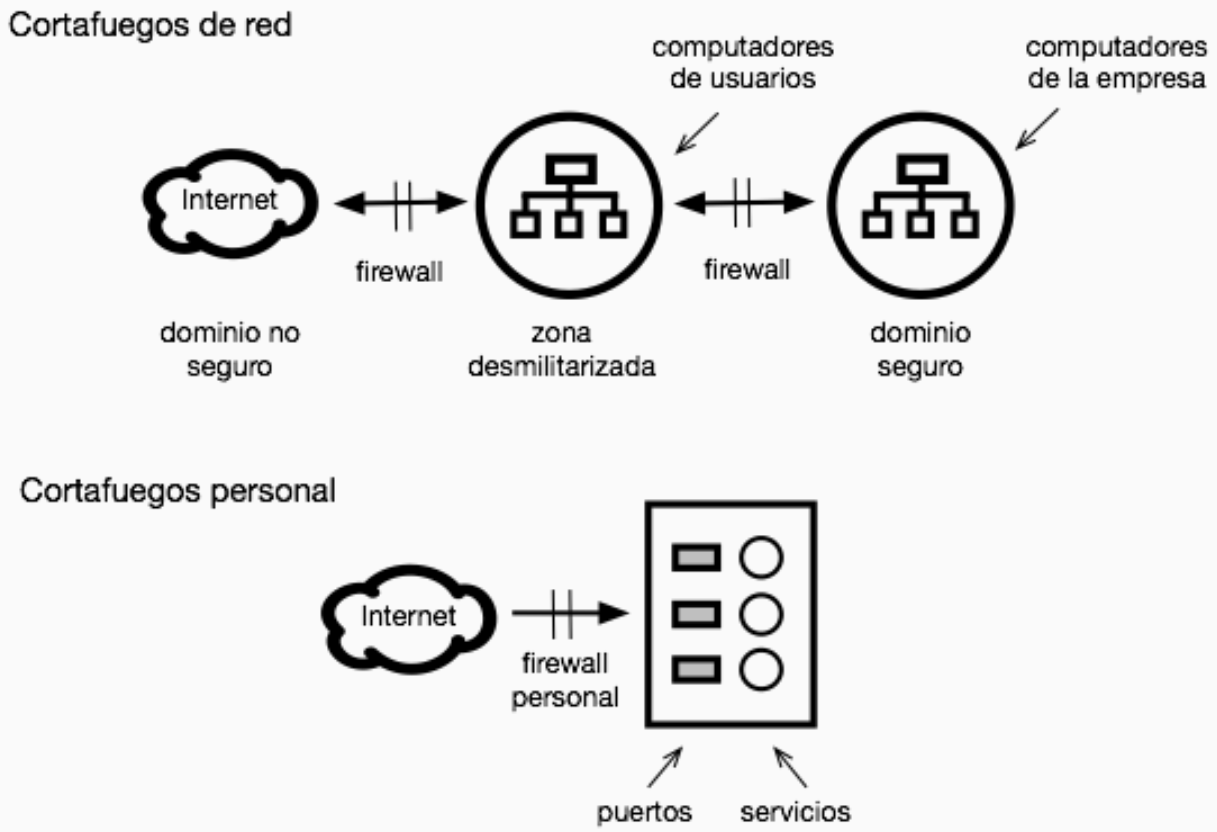

Figure 14:

Cortafuegos para proteger los sistemas y redes

Un cortafuegos de red permite dividir la red en múltiples dominios. Una implementación habitual define varios dominios distintos

- el dominio no seguro constituido por Internet
- otro dominio semi-seguro, denominado zona desmilitarizada
- tercer dominio formado por las computadoras de la empresa

Cortafuegos para proteger los sistemas y redes

Los propios cortafuegos deben ser seguros y resistentes a los ataques; de otro modo, su capacidad para dotar de seguridad a las conexiones puede verse comprometida.

- Además, los cortafuegos no impiden los ataques de tipo túnel, es decir, los ataques contenidos dentro de protocolos o conexiones que el cortafuegos permita.
- Otra vulnerabilidad de los cortafuegos es la suplantación, que es un ataque en el que un host no autorizado pretende ser un host autorizado, cumpliendo algunos de los criterios de autorización.

Cortafuegos para proteger los sistemas y redes

Además de los cortafuegos de red más comunes, existen otras clases de cortafuegos más novedosas:

- cortafuegos personal: es una capa de software incluida en el sistema operativo o se añade como una aplicación. En lugar de limitar la comunicación entre dominios de seguridad, limita la comunicación a (y posiblemente desde) un determinado host.
- proxy de aplicación: un cortafuegos de este tipo entiende y monitoriza los protocolos que utilizan las aplicaciones a lo largo de la red. Un proxy acepta una conexión de la misma forma en que lo haría un servidor determinado y luego inicia una conexión con el servidor de destino original, desactivando comandos ilegales.

Cortafuegos para proteger los sistemas y redes

- cortafuegos XML: tiene el propósito específico de analizar el tráfico XML y de bloquear el código XML no permitido o mal definido.
- cortafuegos de llamadas al sistema: éste se ubica entre las aplicaciones y el kernel, monitorizando la ejecución de las llamadas al sistema.

Clasificaciones de seguridad informática

Existen cuatro clasificaciones de seguridad para los sistemas: A,B,C y D.

- La clasificación de nivel más bajo es la división D, o protección mínima.
- La división D incluye sólo una clase y se usa para los sistemas que no cumplan los requisitos de ninguna de las otras clases de seguridad.

Clasificaciones de seguridad informática

La división C proporciona una protección discrecional y mecanismos de atribución de responsabilidad a los usuarios, mediante el uso de las capacidades de auditoría. La división C tiene dos niveles C1 y C2.

- Un sistema de clase C1 incorpora algún tipo de controles que permiten a los usuarios proteger información privada e impedir a otros usuarios la lectura o la destrucción accidental de sus datos.
- Un entorno C1 es aquél en el que una serie de usuarios cooperantes acceden a un conjunto de datos con el mismo nivel de confidencialidad.

Referencia bibliográfica

A.SILBERSCHATZ, P. GALVIN, y G. GAGNE, Operating Systems Concepts, Cap.16, 9a Edición, John Wiley, 2013.