UNIVERSIDAD NACIONAL

DE

TRUJILLO

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

MONOGRAFIA

Presentada por:

Cárdenas Iglesias, Jean Marcos

Lecca Rengifo, Luis Rolando

Paz Medrano, Harrison Jordi

Vigo Chávez, Daniel Josías

Trujillo – Perú

2021

MONOGRAFIA

Seguridad y protección del sistema de archivos.

Tipos de ataque.

Comprobación de la identidad del usuario.

Control de acceso.

Contenido

INTRODUCCION

La seguridad informática es un tema al que mucha gente no le da la importancia que realmente tiene; muchas veces por el hecho de considerar que es inútil o que jamás la utilizara. Pero en el mundo moderno, cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores. La seguridad es un factor imprescindible en todos los ámbitos profesionales y en la informática, es especialmente importante porque en los ordenadores es donde está almacenada la información confidencial de una empresa o de cualquier otro particular.

El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas. Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a usted es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros.

Capítulo 1: SEGURIDAD Y PROTECCION DEL SISTEMA DE ARCHIVOS

1.1 ¿Qué es seguridad de datos?

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización.

1.2 Amenazas de seguridad:

La seguridad es la situación en la que se está adecuadamente protegido contra pérdidas, de modo tal que los hechos adversos están apropiadamente impedidos, disuadidos, prevenidos, detectados o corregidos. Un sistema seguro no es impenetrable; más bien, es un sistema que se encuentra protegido a un costo justificable, dado la naturaleza de las contingencias o amenazas a las que se halla expuesto. Las medidas de seguridad siguientes están dirigidas a conservar la integridad, disponibilidad y confidencialidad de la información y la autenticación que requiere el sistema de información.

- Confidencialidad: Requiere que la información de un sistema informático solo se encuentre accesible para lectura para aquellas partes que este autorizadas a este tipo de acceso.
- Integridad: Requiere que los contenidos de un sistema informático solo podrán modificarse por las partes que se encuentran autorizadas.
- Disponibilidad: Requiere que los componentes de un sistema informático estén disponibles para todas aquellas partes autorizadas.
- Autenticación: Requiere que el sistema informático sea capaz de verificar la identidad de los usuarios.

Capítulo 2: TIPOS DE ATAQUE

Para comprender los diferentes peligros existentes a nivel de seguridad, es necesario comenzar por la definición de los requisitos de seguridad. La seguridad de los sistemas informáticos y de la red va dirigida a cuatro requisitos básicos:

- Confidencialidad. Requiere que la información de un sistema informático sólo se encuentre accesible para lectura para aquellas partes que estén autorizadas a este tipo de acceso. Este tipo de acceso incluye impresión, mostrado de datos y otras formas de observación, incluyendo la simple revelación de la existencia de un elemento.
- Integridad. Requiere que los contenidos de un sistema informático sólo podrán modificarse por las partes que se encuentran autorizadas. Las modificaciones incluyen escritura, cambio, modificación del estado, borrado y creación.
- Disponibilidad. Requiere que los componentes de un sistema informático estén disponibles para todas aquellas partes autorizadas.
- Autenticación. Requiere que el sistema informático sea capaz de verificar la identidad de los usuarios.

2.1 Tipos de peligros

Los tipos de ataques contra la seguridad del sistema o de la red se clasifican mejor considerando las funciones de un sistema informático como si se tratase de un proveedor de información. En general, existe un flujo de información desde una fuente, pudiéndose tratar de un fichero o una región de memoria, a un destino, que puede ser otro fichero o puede ser el mismo usuario. Ese flujo virtual se muestra en la ilustración 3. El resto de elementos de la figura muestran las siguientes cuatro categorías generales de ataques:

- **Interrupción**. Se destruye un componente del sistema o se encuentra no disponible o utilizable. Es un ataque centrado en la disponibilidad. Ejemplos de este tipo incluyen la destrucción de una pieza del hardware, como un disco duro,

la interrupción del canal de comunicación o la eliminación del sistema gestor ficheros.

- **Intercepción**. Una parte no autorizada consiga acceso a un componente. Esto es un ataque dirigido hacia la confidencialidad. La parte no autorizada puede ser una persona, un programa o un ordenador. Ejemplos de este estilo son la escucha en un canal de comunicación para capturar datos y la copia ilícita de ficheros o programas.
- **Modificación**. Un elemento no autorizado no sólo tiene acceso a un componente, sino que también es capaz de modificarlo. Éste es un ataque que va dirigido hacia la integridad. Los ejemplos incluyen cambiar valores de un fichero de datos, alterar un programa para que exhiba un comportamiento diferente, y modificar el contenido de los mensajes que se transmiten por la red.
- **Fabricación**. Un elemento no autorizado inserta objetos extraños en el sistema. Estos son ataques contra la autenticación. Ejemplos de este tipo son la inserción de mensajes externos en una red o la inclusión de un registró en un fichero.

Ilustración 1: Ámbito de la seguridad informática.

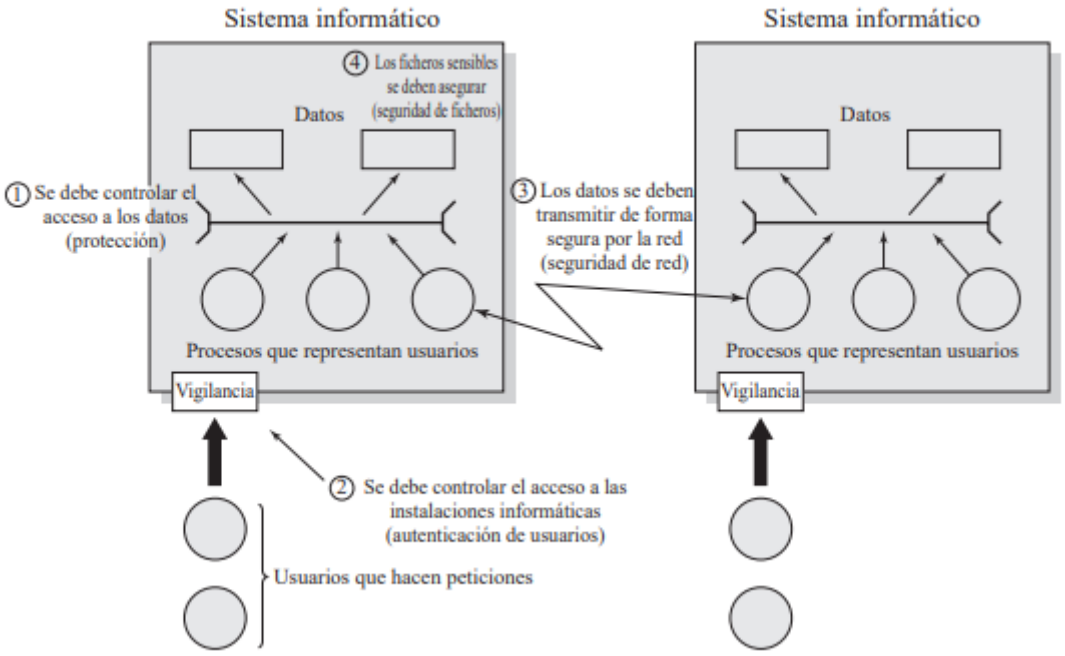
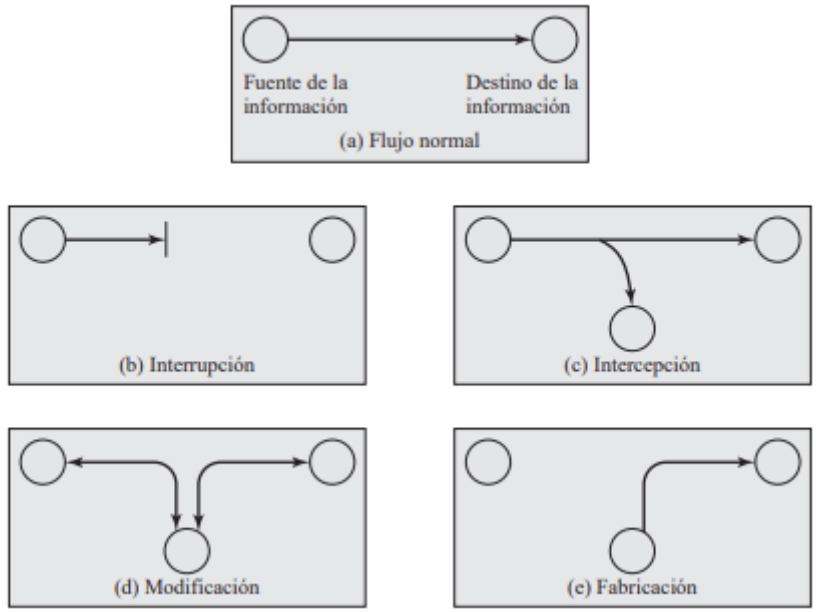


Ilustración 2: Peligro de seguridad



2.2 Componentes de un sistema informático

Los componentes de un sistema informático se pueden clasificar en hardware, software, datos y líneas de comunicaciones y red. En la ilustración 2 se indica la naturaleza de los peligros que afectan a cada una de estas categorías. A continuación, revisaremos cada una por separado.

Tabla 1: Peligros de seguridad y componentes

	Disponibilidad	Privacidad	Integridad/Autenticación
Hardware	Equipamiento robado o deshabitado, por lo tanto denegación de servicio.		
Software	Borrado de programas, denegación de acceso a los usuarios.	Copia no autorizada de software.	Modificación de un programa, bien para hacer que falle durante la ejecución o para que realice una tarea diferente.
Datos	Borrar ficheros, denegación de acceso a los usuarios.	Lectura no autorizada de datos. Un análisis estadístico de los datos que revele la información subyacente.	Modificación de los ficheros existentes o creación de nuevos ficheros.
Líneas de comunicación	Borrado o destrucción de mensajes. Las líneas de comunicación o redes no se encuentran disponibles.	Lectura de mensajes. Observación de los patrones de tráfico de mensajes.	Modificación, borrado, reordenación o duplicación de mensajes. Fabricación de mensajes falsos.

- **Hardware**. El principal peligro del hardware de un sistema informático se encuentra en el área de la disponibilidad. El hardware es el componente más vulnerable a ataques y también es el menos accesible a una manipulación remota. Los principales peligros incluyen daño accidental o deliberado a los equipos, así como el robo. La proliferación de ordenadores personales y estaciones de trabajo y el in- cremento en el uso de redes de área local incrementan las potenciales pérdidas en esta área. Para ha- cer a frente estos peligros se necesitan medidas de seguridad física y administrativa.
- **Software**. Lo que hace del hardware del sistema informático algo útil para negocios e individuos son el sistema operativo, las utilidades y los programas de aplicación. Existen diferentes tipos de peli- gros a tener en cuenta.

  Un peligro importante en relación al software es el referente a la disponibilidad. El software, es parcialmente el software de aplicación, es a menudo fácil de borrar. De la misma forma, también pue- de verse alterado o dañado hasta dejarlo inservible. Para mantener una alta disponibilidad, resulta necesaria una gestión de la configuración del software cuidadosa, que incluya realización de copias de respaldo (*backups*) y actualización a las versiones más recientes del software. Una cuestión más complicada es la referente a la modificación del software que hace que el programa sigua funcionando pero que su comportamiento sea diferente al que realizaba anteriormente, lo cual implica un peligrode integridad y autenticación. Los virus informáticos y los ataques similares se encuentran dentro de esta categoría y se tratarán más adelante en este capítulo. El último problema es el relativo a la privacidad. A pesar de que existen diferentes medidas disponibles, el problema de la copia no autorizada de software aún no se encuentra resuelto.
- **Datos**. La seguridad relativa al hardware y al software se encuentra habitualmente dentro de los cometidos de los profesionales de administración del sistema informático, o en el caso de pequeñas instalaciones, en los propietarios de ordenadores personales. Un problema mucho más amplio es el relativo a la seguridad de los datos, o que incluye los ficheros y cualquier otro tipo de datos controlados por los individuos, grupos, u organizaciones.

Los aspectos de seguridad relativos a los datos son muy amplios, incluyendo la disponibilidad, la privacidad y la integridad. El caso de la disponibilidad, se centra en la destrucción de ficheros de da- tos, que puede ocurrir de forma accidental o maliciosa.

Un aspecto evidente en lo concerniente a la privacidad es, por supuesto, la lectura no autorizada de ficheros de datos o bases de datos, y en esta área se han volcado mayor cantidad de esfuerzos e investigación que en cualquiera otra área de la seguridad informática. Un peligro menos obvio para la privacidad incluye el análisis de datos, y se manifiesta en el uso de, las así llamadas, bases de datos estadísticas, que contienen información resumida o agregada. Presumiblemente, la existencia de in- formación agregada no es un peligro para la privacidad de los individuos. Sin embargo, a medida que crece el uso de las bases de datos estadísticas, existe un incremento potencial de la filtración de información personal. En esencia, las características de individuos concretos se pueden identificar a través de un análisis minucioso. Por poner un ejemplo sencillo, si un registro de una tabla agregada incluye los ingresos correspondientes a A, B, C, y D y otro registro suma los ingresos de A, B, C, D, y E, la diferencia entre los dos valores sería los ingresos de E. Este problema se acrecienta con el creciente deseo de combinar conjuntos de datos. En muchos casos, el cruce de diversos conjuntos de información hasta los niveles apropiados de relevancia para un problema determinado, implican descender hasta nivel de unidades elementales para poder construir los datos necesarios. De esta forma, las unidades elementales, que sí están sujetas a consideraciones de privacidad, se encuentran disponibles en diferentes pasos del proceso de estos conjuntos de datos.

Para finalizar, la integridad de datos es un aspecto clave en muchas instalaciones. La modificación de los ficheros de datos puede llevar a una serie de consecuencias que van desde problemas menores hasta desastrosos.

- **Líneas de comunicaciones y redes**. Un mecanismo útil para la clasificación de los ataques de seguridad a la red es en base a los términos de ataques pasivos y ataques activos. Un ataque pasivo intenta aprender o hacer uso de la información del sistema, pero no afecta a los recursos del mismo. Un ataque activo intenta alterar los recursos del sistema o afectar a su operativa.

Los ataques pasivos son el espionaje o la monitorización de las transmisiones. El objetivo del oponente es obtener información de qué se está transmitiendo. Los dos tipos de ataques pasivos son la lectura de los contenidos de los mensajes y el análisis de tráfico.

- **La lectura de los contenidos de los mensajes** visualizar la ilustración 4. Una con- versación telefónica, un mensaje de correo electrónico o la transferencia de un fichero pueden contener información sensible y confidencial. Sería deseable evitar que cualquier oponente tenga acceso a los contenidos de estas transmisiones.
- Un segundo tipo de ataques pasivos, los **ataques de análisis de tráfico**, son más discretos visualizar la ilustración 5. Supongamos que tenemos un mecanismo para ocultar los contenidos de los mensajes u otro tráfico de información de forma que los oponentes, intrusos si capturan los mensajes, no puedan ex- traer la información que contiene. La técnica habitual para ocultar estos contenidos es el cifrado. Si queremos una protección basada en cifrado funcionando, un oponente aún podría observar cuáles son los patrones de estos mensajes. El oponente podría determinar la ubicación e identidad de los ordena- dores que se comunican y podría observar la frecuencia y objeto de los mensajes que se intercambian. Esta información puede resultar útil para adivinar la naturaleza de las comunicaciones que se están llevando a cabo.

Los ataques pasivos son muy difíciles de detectar debido a que no implican ninguna alteración delos datos. Habitualmente, el tráfico de mensajes se envía y recibe de una manera aparentemente normal y ni el emisor ni el receptor se dan cuenta de que un tercer elemento ha leído los mensajes o analizado los patrones de tráfico.

Sin embargo, es posible prevenir estos ataques, habitualmente por me- dio de cifrado. De esta forma, el énfasis que se hace sobre los ataques pasivos se centra en su prevención más que en su detección.

Ilustración 3: Lectura de los contenidos de los mensajes

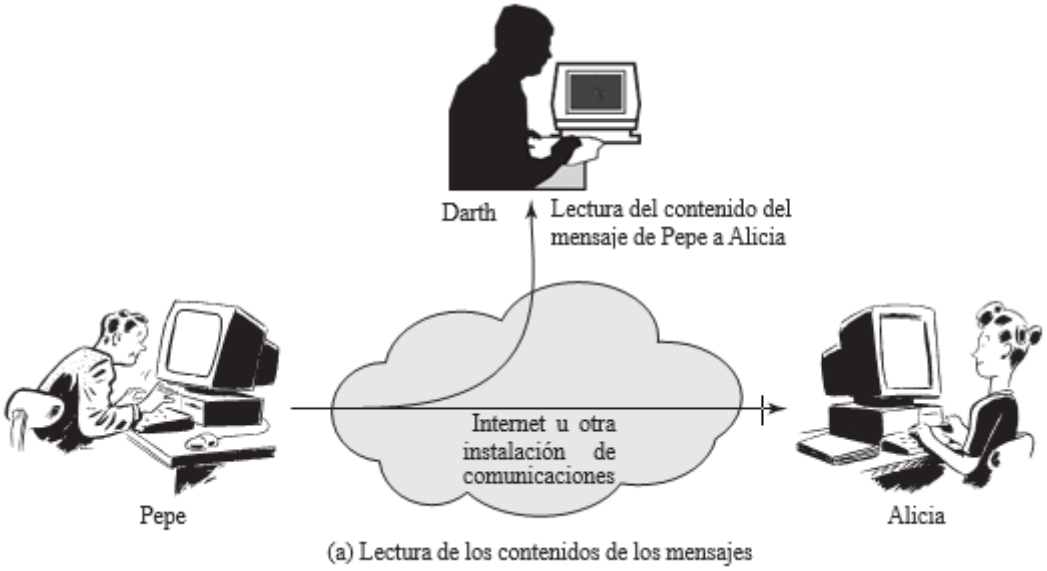
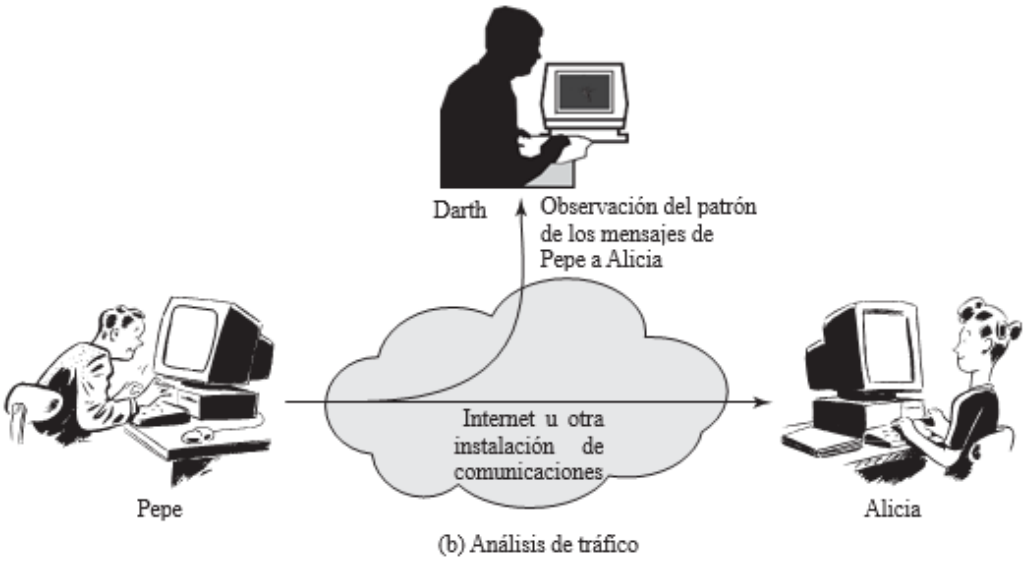
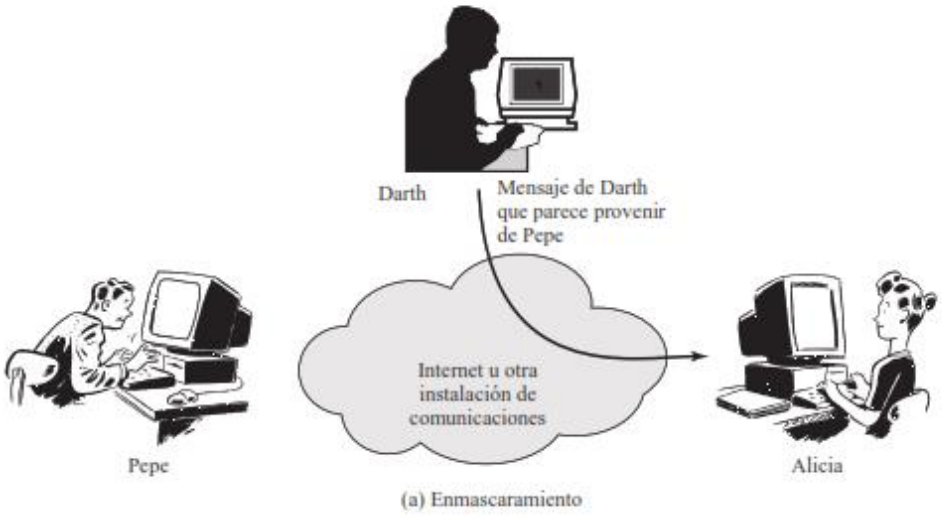


Ilustración 4: Análisis de trafico



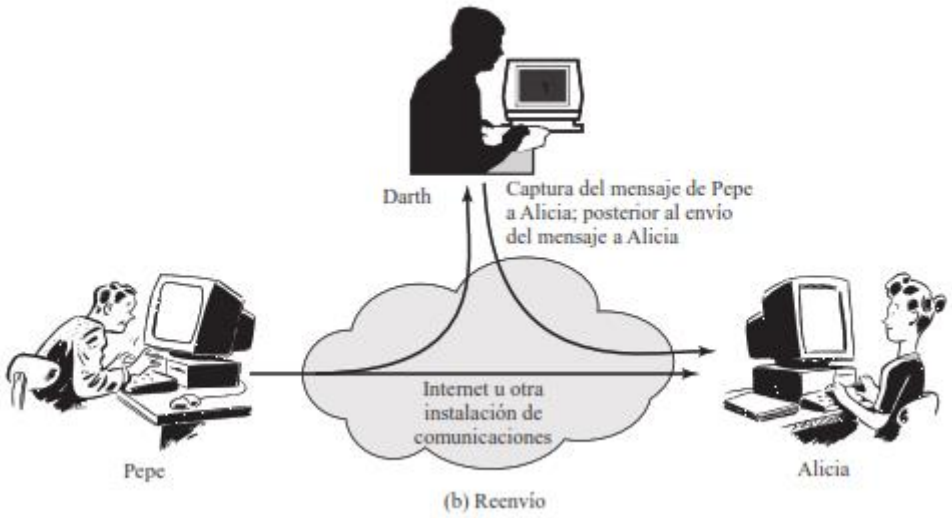
Los ataques activos implican algunas modificaciones en el flujo de datos o la creación de flujos de datos falsos y se pueden subdividir en cuatro diferentes categorías: enmascaramiento, reenvío, modificación de mensajes y denegación de servicio.

- **El enmascaramiento** ocurre cuando el elemento intenta hacerse pasar por otro diferente. Un ataque de enmascaramiento incluye habitualmente una de las otras formas de ataques activos. Por ejemplo, se pueden capturar las secuencias de autenticación y reenviarla posteriormente, después de que se haya intercambiado una secuencia válida, de forma que permita a un elemento con pocos privilegios obtener privilegios extra, suplantando a otro que los posea.



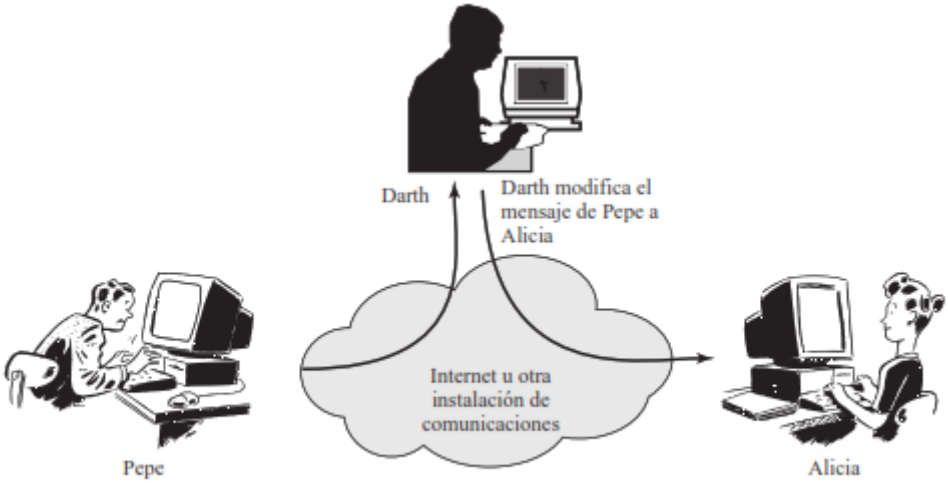
(a) Enmascaramiento

- **El reenvío** implica la captura pasiva de una unidad de datos y su posterior retransmisión para producir un efecto no autorizado.



(b) Reenvío

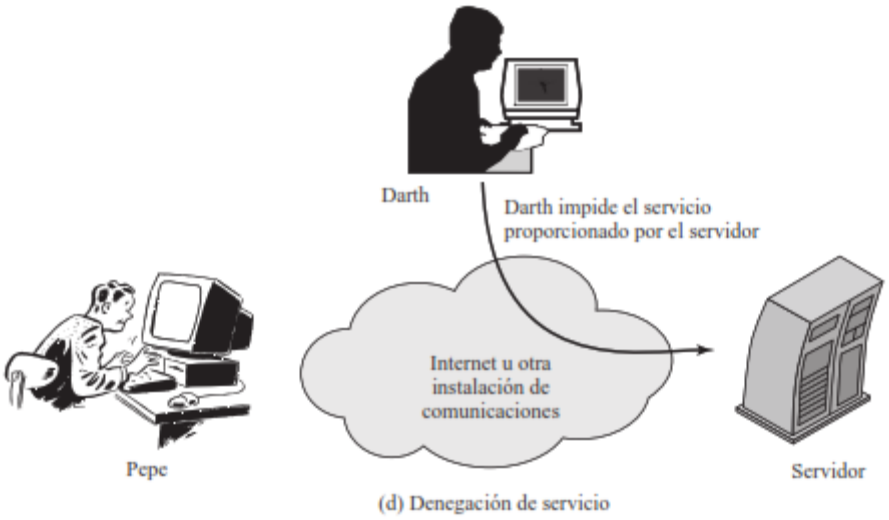
- **La modificación de mensajes** significa sencillamente que una parte de un mensaje válido se ha alterado, o que los mensajes se han borrado o reordenado, para producir un efecto no autorizado. Por ejemplo, si se modifica un mensaje cuyo significado es «Permite a Pepe Pérez leer el fichero confidencial de cuentas» para que diga «Permite a Juanito Sánchez leer el fichero confidencial de cuentas».



(c) Modificación de mensajes

- La **denegación de servicio** previene o imposibilitar el uso normal o la gestión de las instalaciones de comunicaciones. Este ataque puede tener un objetivo específico; por ejemplo, un elemento puede suprimir todos los mensajes dirigidos a un destino en particular (por ejemplo, el servicio

de auditoría de seguridad). Otra forma de denegación de servicio es la desarticulación de toda la red, bien deshabilitándola o sobrecargándola con mensajes para degradar su rendimiento.



(d) Denegación de servicio

- Los ataques activos presentan características opuestas a los ataques pasivos. Mientras que los ataques pasivos son difíciles de detectar, sí existen medidas que permiten evitar su éxito. Por otro lado, es bastante más difícil prevenir los ataques activos de forma completa, debido a que para poder hacerlo se requerirían protecciones físicas para todas las instalaciones de comunicaciones y todas las rutas. Sin embargo, el objetivo en este caso es la detección de dichos ataques y la recuperación de cualquier efecto o retraso que pudieran causar. Debido a que la detección tiene un efecto disuasorio, también esto contribuye a su prevención.

Capítulo 3: COMPROBACIÓN DE LA IDENTIDAD DEL USUARIO.

Es la protección de una persona tiene a su espacio en un SO o software, donde tiene guardado sus datos, permitiéndole así evitar que personas secundarias tengan fácil acceso a ellos o accedan sin el permiso de ella.

Esta forma consta de requisitos para poder verificarlo, ya sea mediante su aspecto físico, forma de hablar, etc. Haciéndolo complejo su acceso para una computadora, siendo el objetivo del sistema de identificación no es el de identificar, sino autenticar es quien dice ser. Debido que para el sentido común humano estos términos pueden significar lo mismo, pero esto no aplica a la lógica de la computadora.

Los métodos que se pueden aplicar suelen dividirse en 3 grandes categorías:

a) Lo que el usuario sabe.
b) Lo que el usuario posee.
c) Una característica física del usuario o acto involuntario (autenticación biométrica).

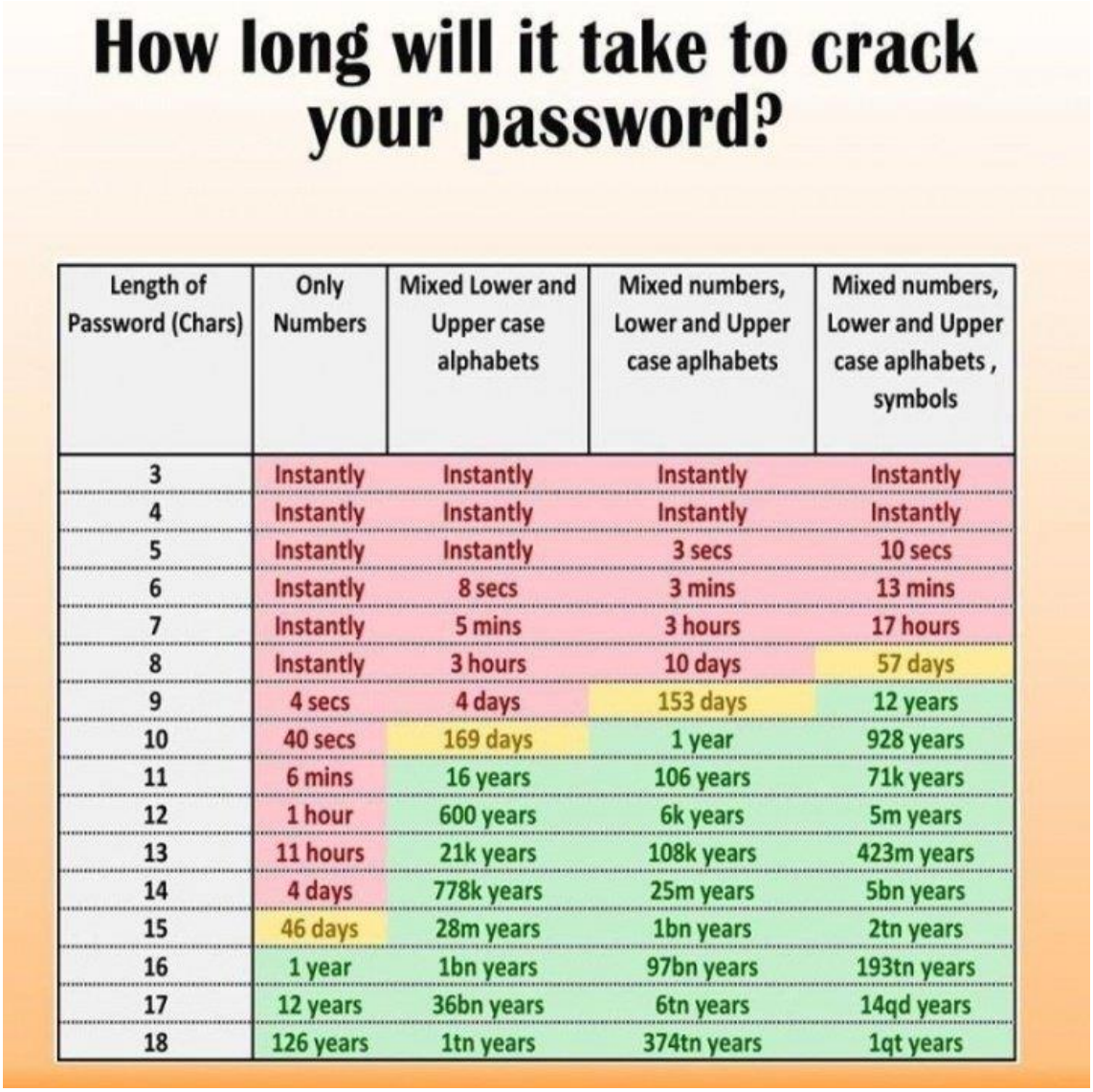
Tipo de sistemas basados:

3.1 Contraseñas

Lo más básico que todos conocemos, es simplemente basándose en una prueba de conocimiento al usuario que a priori él puede superarla.

Tiempo que se demorarían en hackear o crakear una contraseña.

Ilustración 5: Password



How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

3.2 Tarjetas inteligentes

En 1970, Roland Moreno creaba la integración de un procesador en una tarjeta de plástico (chipcard), abriendo así un abanico de posibilidades en cuestión a la autenticación del usuario.

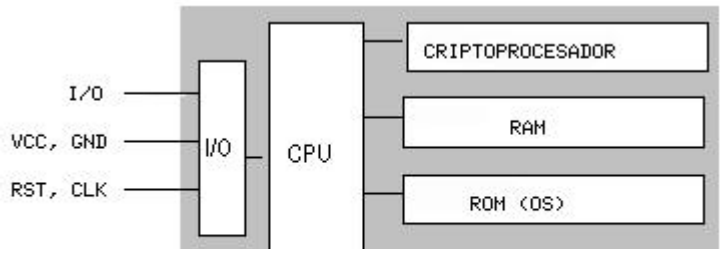


Ilustración 6: tarjetas inteligentes

Esta innovación permitió que sea resistente a la adulteración ofreciendo funciones de almacenamiento seguro de información y el proceso de esta misma en base a tecnología VLSI.

Tipos de TI:

Según su SO.

De memoria: solo contienen ficheros, las aplicación no son ejecutable. Su sistema operativo es limitado, haciendo uso de comando básicos de lectura y escritura.

Con aplicaciones: es todo lo contrario a las TI de memoria, por que su sistema operativo cuenta con comandos y APIs de programación.

JAVA Card: llevan una pequeña maquina virtual JAVA (JVM) lo que le permite ejecutar aplicaciones java.

Según su interfaz.

De contacto: tienen que ser insertadas a un lector para poder brindar la información del usuario almacenado en ella y cumplir su función.

Sin contacto: emplea la misma funcionalidad de la TI de contacto, pero el protocolo de esta es diferente para la transmisión de información, permitiendo asi evitar el contacto físico con el lector.

Hibrida: TI sin contacto a la que se le asigna un según chip de contacto.

Dual: tiene la función de las TI de contacto y sin contacto, pero con un circuito integrado.

Según sus capacidades.

De memoria: se usan en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.

Microprocesadas: suelen ser usadas para identificación y pago con monederos electrónicos.

Criptográficas: incorporan modulos hardware para que puedan ejecutar algoritmos usados en cifrados y firmas digitales, almacenando de forma segura un certificado digital y clave privada.

Ventajas: tiene incorporado un hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado, además su uso es factible tanto en control de acceso físico como lógico.

Desventajas: el coste adicional para una organización el comprar y configurar la infraestructura del dispositivo de lectores y las tarjetas propias, además de que se pueda perder fácilmente y en ese lapso de tiempo no se disponga de ella.

3.3 Autenticación biométrica

Basada en las características físicas del usuario a identificar. El reconocimiento de formas, la IA y el aprendizaje son las ramas de la informática que desempeñan este papel muy importante en los sistemas de identificación biométricos, la criptología aquí tiene un uso limitado y secundario, como el cifrado de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos.

Partes importantes:

Captura o lectura de los datos que el usuario a validar presenta.

Extracción de ciertas características de la muestra.

Comparación de tales características con las guardadas en una base de datos.

Decisión de si el usuario es válido o no. Fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de **falso rechazo** (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de **falsa aceptación** (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada

genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Ilustración 7: Autenticación biométrica

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándars	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 1997 (USD)	5000	5000	1200	2100	1000	1200

3.3 Verificación de voz

Si usuario desea acceder al sistema tendrá que pronunciar unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer.

Enrolamiento y verificación:

Se debe de capturar y enrolar una muestra de información biométrica de voz en un micrófono para poder crear una plantilla de referencia a fin de poder comparar muestras para futuros intentos de autenticación.

Se comparan las siguientes cualidades:

Duración.

Intensidad.

Dinámica.

Tono.

La principal desventaja del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos.

3.4 Verificación de huellas

Si el usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas (en la figura podemos ver una imagen de una huella digitalizada con sus minucias). Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario.

Ilustración 8

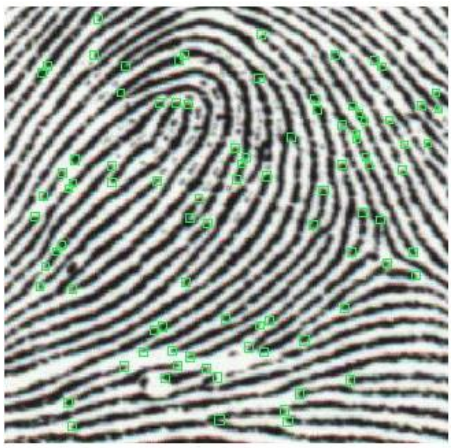


Figura 8.2: Huella dactilar con sus minucias extraídas. ©1998 Idex AS, http://www.idex.no/.

3.5 Verificación de patrones oculares

se dividen en 2 tipos de tecnología:

- Retina
- Iris

Para este tipo de medida la probabilidad en el mundo de una posible coincidencia es casi 0, además de que una vez fallecido el usuario el acceso a su espacio digital es difícil de hackear mediante la falsa aceptación.

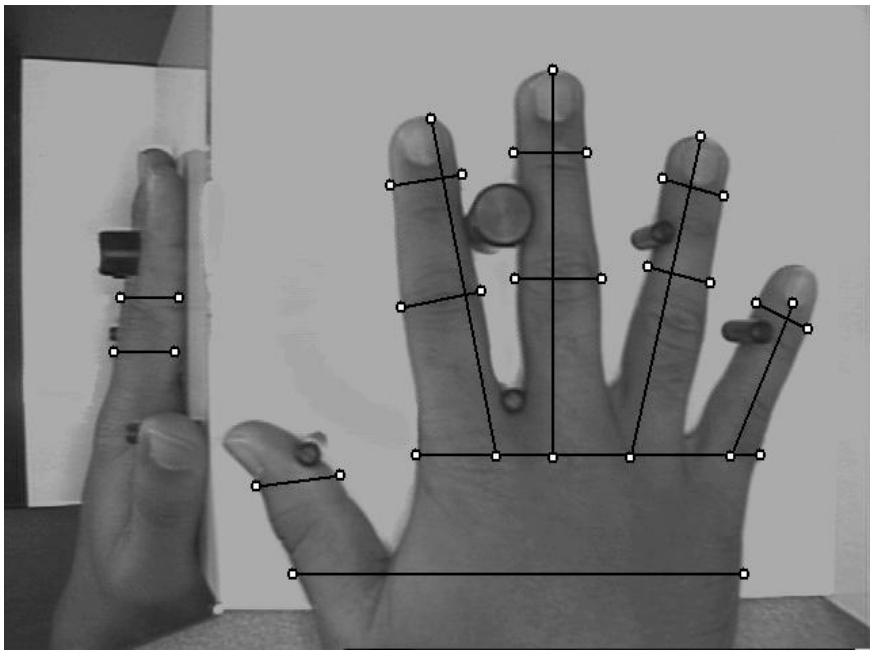
La principal desventaja es su escasa aceptación, debido a su difícil comodidad para el usuario, además de que estos no se fían de un haz de rayos analizando su ojo, y otra es el motivo de ocultar posibles enfermedades que pueda arrojar al momento de hacer un examen ocular.

3.6 Verificación geométrica de la mano

Cuando el usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad.

Ilustración 9: verificación geométrica de la mano



3.7 Verificacion para usuarios en UNIX

Clásica: los datos ingresados tanto login como contraseña se almacenan en el fichejo /etc/passwd, conteniendo la información necesaria para permitir a los usuarios conectarse con el sistema y trabajar.

Capítulo 4: CONTROL DE ACCESO.

El control de acceso define a qué objetos puede acceder cada sujeto. Un objetivo es cualquier entidad que contenga información. Los sujetos acceden a los objetos, y pueden ser usuarios, procesos, programas u otras entidades.

4.1 Matriz de control de acceso:

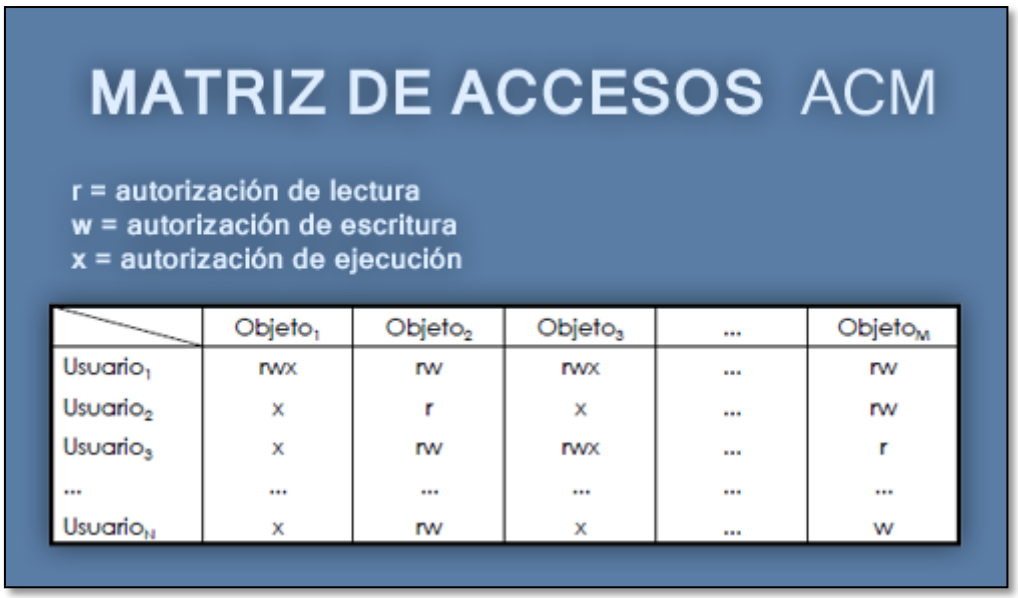
Es un modelo abstracto formal de seguridad que caracteriza los permisos de cada sujeto con respecto a todos los objetos del sistema.

Tabla 2: objetivo dominio

objeto / dominio	F_1	F_2	F_3
D_1	ejecutar	-	escribir
D_2	ejecutar	leer	ejecutar
D_3	ejecutar	-	-

Las filas de la matriz representan dominios y las columnas objetos. La entrada de acceso (i, j), define el conjunto de operaciones que un sujeto en el dominio D puede invocar con el objeto O.

Tabla 3: Matriz de acceso



4.2 Políticas de control de acceso:

Una política de control de acceso es un conjunto de reglas o permisos que buscan preservar las propiedades de la seguridad de información: Integridad, Confidencialidad, Disponibilidad, etc.

Existen 3 políticas de control de acceso:

- Control de acceso discrecional (RAC)
- Control de acceso obligatorio (MAC)
- Control de acceso basado en roles (RBAC)

4.3 Control de acceso discrecional (RAC)

Este tipo de control de acceso consiste en que el creador de los objetos es el que determina el acceso a dichos objetos.

Se basa en 2 conceptos fundamentales:

- **Propietario:** Todo objeto en el sistema tiene un propietario.
- **Derechos de acceso y permisos:** Un propietario puede asignar permisos a otros sujetos.

Se implementa mediante:

- **Bits de permisos:** Se especifica a un usuario como el propietario de un archivo, y cada archivo o directorio se afilia a un grupo. Se otorgan permisos de lectura, escritura o ejecución. En un momento dado un usuario pertenece a un grupo y adquiere los derechos de ese grupo.
- **Sistema de contraseñas:** El propietario asigna a cada archivo una contraseña.
- **Lista de capacidades:** Cada objeto tiene un solo propietario, el cual otorga o cancela privilegios a los demás sujetos sobre dicho objeto.
- **Listas de control de acceso:** Los archivos y directorios tienen conjuntos de permisos configurados para el propietario del archivo, el grupo asociado con el archivo y todos los otros usuarios del sistema. Sin embargo, estos permisos tienen sus limitaciones. Por ejemplo, no se pueden configurar diferentes permisos para usuarios diferentes. Una lista de control de acceso es un conjunto de entradas de usuario, grupo y modo asociado a un archivo que especifica los

permisos de acceso para todas combinaciones posibles de identificación de usuario o identificación de grupo.

4.4 Permisos

En Unix la seguridad de los diferentes objetos del sistema viene determinado por usuario y el grupo. Internamente, estas entidades el sistema las representa a través de dos números (credenciales), el uid - user id, para el usuario - y el gid - group id, para el grupo -, que representa a un conjunto de usuarios. Cada usuario pertenece a un grupo primario y puede pertenecer a varios grupos secundarios. Los permisos que pueden existir sobre los objectos del sistema de ficheros son:

- **Permiso de Lectura (R).**
- **Permiso de Escritura (W).**
- **Permiso de Ejecución (X).**
- **Permiso setuid.**
- **Permiso setgid.**

En Windows tenemos permisos parecidos: Control Total, Modificar, Lectura, Escritura, etc.

```
user::rw-
user:lisa:rw-          #effective:r--
group::r--\\
group:toolies:rw-      #effective:r--
mask::r--\\
other::r--\\
```

4.5 Control de acceso obligatorio (MAC):

MAC es un tipo de control de acceso definido por el TCSEC que consiste en restringir el acceso a los objetos en función de la" sensibilidad" (representada por una etiqueta) de la información contenida en dichos objetos. Su característica más importante es que es la política de seguridad del sistema la única que determina el acceso a los objetos, retirándole este privilegio al creador de los objetos.

MAC es usada en sistemas multinivel que procesan datos altamente confidenciales, como información clasificada gubernamental o militar. Un sistema multinivel es aquel que maneja múltiples niveles de clasificación entre sujetos y objetos.

- **Etiquetas:** En un sistema basado en MAC, todos los sujetos y objetos deben tener una etiqueta asignada. Para acceder a un objeto, el sujeto debe tener un valor de etiqueta igual o mayor que dicho objeto.
- **Importación y exportación de datos:** Controlar dicho flujo de información de y para otros sistemas es una función crítica de los sistemas basados en MAC. Deben asegurar que las etiquetas son mantenidas de forma adecuada.

4.6 Control de acceso basado en roles (RBAC):

Los permisos para realizar ciertas operaciones son asignados a roles específicos. Los usuarios son asignados a roles particulares, a través de los cuales adquieren permisos para realizar funciones particulares. RBAC se diferencia de las ACLs usadas por los sistemas discrecionales en que asigna permisos a operaciones específicas con significado en la organización, en lugar de a objetos de datos de bajo nivel. Por ejemplo, una lista de control de acceso puede ser usada para permitir o denegar el acceso a un fichero, pero no se le podría decir en que formas puede ser modificado dicho fichero. Además, el uso de roles como medio para asignar privilegios a usuarios simplifica en gran medida el manejo y creación de usuarios. El uso de RBAC para manejar privilegios de usuario está muy extendido. Sistemas como Microsoft Active Directory, SELinux, FreeBSD, Solaris, Oracle DBMS, PostgreSQL 8.1, SAP R/3 implementan alguna forma de RBAC

Conclusiones

La seguridad de un sistema incluye la protección ante posibles daños físicos de los datos hasta el acceso indebido a los mismos, ataques contra la confidencialidad, la integridad o la disponibilidad de recursos en un sistema deben prevenirse y solventarse mediante la política y los mecanismos de seguridad de un sistema. De nada sirve tener mecanismos de protección buenos, si el SO no es capaz de identificar a los usuarios que acceden al sistema o si no existe una política que salvaguarde datos ante la rotura de un disco.

Es necesario comprobar que los recursos solo se usan por aquellos usuarios que tienen derechos de acceso a los mismos. Las políticas de protección y seguridad de hardware, software y datos deben incluirse dentro del SO pudiendo afectar a uno o varios componentes del mismo.

Bibliografía

- Stallings, W. (2005). *Sistemas Operativos: Aspectos Internos y Principios de Diseño (5ª Ed.).* Alhambra. doi:8420544620
- Romero LA. Seguridad de Autenticación. Segunda ed. Silverio FAyB, editor. Lima: Publicación en Libro; 2006
- Ardita JC. Autorización en Sistema. Primera ed. Silverio FALyB, editor. Ecuador: Revista; 2013.
- Autenticación de usuarios: https://www.rediris.es/cert/doc/unixsec/node14.html
- Gracia Fernández López (2007). Seguridad en sistemas operativos: Seguridad en sistemas de información: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/03%20-%20Seguridad%20en%20Sistemas%20Operativos.pdf
- Propuesta de seguridades para los servidores web y correo electrónico bajo plataforma Linux, de la Comandancia General de la Fuerza Terrestre ubicada en la ciudad de Quito. CAPITULO 2: http://repositorio.utc.edu.ec/handle/27000/635