Semana 2: Control de Acceso

Control de Acceso

Aprendizajes esperados

Contenidos:

- Técnicas de control de acceso
- Administración del control de acceso
- Control de acceso descentralizado

Técnicas de control de acceso

- El **CONTROL DE ACCESO** constituye una poderosa herramienta para proteger la entrada a un sistema de software, un web completo, a ciertos directorios, a una red, e incluso a archivos o programas individuales.
- Este control consta generalmente de tres pasos: **identificación**, **autenticación** y **autorización**.

Técnicas de control de acceso

- Se denomina **IDENTIFICACIÓN** al momento en que el usuario se da a conocer en el sistema.
- Se denomina **AUTENTICACIÓN** a la verificación que realiza el sistema sobre esta identificación.
- Se denomina **AUTORIZACIÓN** al proceso por el cual se autoriza al usuario identificado y autenticado a acceder a determinados recursos del sistema, red o aplicación.

Técnicas de control de acceso

- La **AUTENTICACIÓN**, por lo tanto, debe preceder la **AUTORIZACIÓN**.
- Por una parte, un adecuado **CONTROL DE ACCESO** nos permite discriminar a quien tenga acceso y a quien no lo tenga.
- No obstante, cuando queremos aplicar el protocolo desde el acceso, la cuestión no se limita a permitir o no la entrada, sino también a saber quién ha entrado y dónde ha de ser ubicado.

Control de acceso con passwords

- Este tipo de control de acceso constituye sin duda la forma más extendida a la que todos los usuarios ya están sobradamente acostumbrados.
- En este caso se requiere que los usuarios introduzcan un nombre y una contraseña como medio de asegurar su identidad.

Control de acceso con passwords

- La mayor parte de los servidores proporcionan esta forma de autenticación, eso sí, con distintas posibilidades y niveles de seguridad implementadas.

Problemas con las passwords

- Las **PASSWORDS** (o **contraseñas**) han sido usadas por años para autenticar a los usuarios de los sistemas y dar acceso a transacciones, pero son inseguras porque:
  - Viajan por la red (usualmente).
  - Son compartidas por 2 partes (usuario y sistema).
  - No generan medios de prueba confiables.

Problemas con las passwords

- Los usuarios requieren conectarse a varios sitios
  - Tienen problemas para recordar muchas **passwords**.
  - Sus **passwords** están tan expuestas como el sitio más expuesto en el que se almacenen.

Problemas con las passwords

- Es sabido que las **PASSWORDS** son uno de los puntos más débiles que existe en la seguridad informática, ya que una mala definición de estas facilita tanto **ATAQUES POR INGENIERÍA SOCIAL** como **ATAQUES BASADOS EN UN DICCIONARIO**.

Problemas con las passwords

- Estos últimos se concretan al combinar una serie de nombres de usuario (o nombres de login) contra una lista de **passwords** hasta acertar, lo que naturalmente requiere de tiempo de operación y conforme pasa el tiempo, más recursos de los equipos involucrados.
- Un **ATAQUE BASADO EN UN DICCIONARIO** es un **ATAQUE DE FUERZA BRUTA**.

Programas de password cracking

- Cain & Abel
- John the Ripper
- THC Hydra
- Aircrack
- Medusa
- Ophcrack
- RainbowCrack & Rainbow Tables
- L0phtcrack

JOHN THE RIPPER

- **JOHN THE RIPPER** es un programa de criptografía que aplica **FUERZA BRUTA** para descifrar contraseñas.
- Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros.
- Es una herramienta de seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de sus usuarios sean suficientemente buenas.

JOHN THE RIPPER

- La siguiente es la sintaxis de uso de **JOHN THE RIPPER**:

```
# john --format=MD5 /etc/shadow
```

```
# john  /etc/shadow
```

```
# john --incremental  /etc/shadow
```

Instalación de JOHN THE RIPPER

Bajar el paquete **john-1.7.6.tar.gz**

```
# tar xvfz john-1.7.0.2.tar.gz
# cd john-1.7.6
# cd src
# make
# make clean linux-x86-any
# cd ../run
# ./john --test
```

Nivel de seguridad de las passwords

- **Password Meter**
- **password strength meter**
- **Ultimate Password Strength Meter**
- **YAPM** (**Yet Another Password M**eter)
- **Password checker** (Propietario Microsoft)

Programas generadores de passwords

- PcTools Password Generator
- Infinite Password Generator
- Perfect Passwords
- IronKey
- Troupware's PassX
- OnePass
- GoodPassword

Identificación biométrica

- Tal y cómo aparecen las investigaciones criminales donde las huellas digitales muchas veces nos llevan a identificar al responsable del delito y al igual que sucede cuando nacemos y somos registrados con nuestra **huella digital**, la **IDENTIFICACIÓN BIOMÉTRICA** se utiliza en las personas.

Identificación biométrica

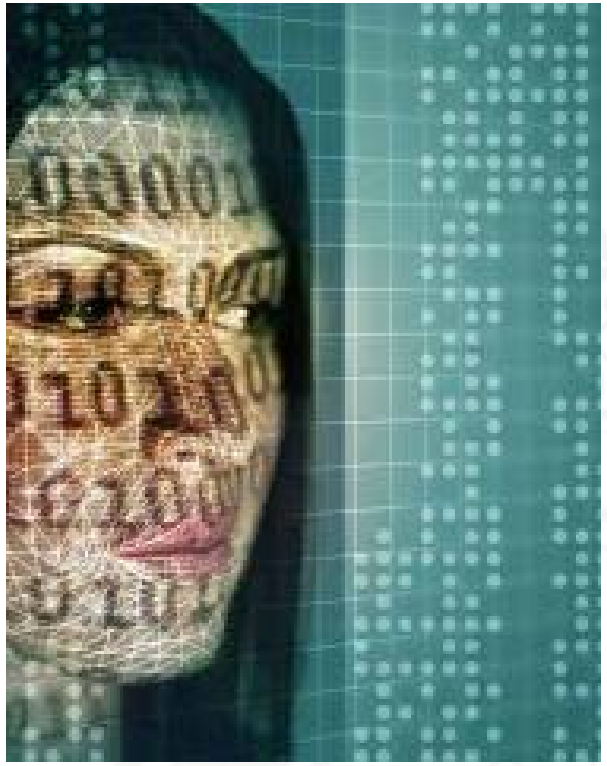
- La utilización de estos **MÉTODOS BIOMÉTRICOS** han llevado a las industrias a crear software y hardware, basando sus sistemas de seguridad a la extracción de puntos característicos de la **huella digital**, con este proceso la información dactilar se ha reducido a un algoritmo matemático.

Identificación biométrica

Identificación biométrica

- Uno de los beneficios de utilizar los **MÉTODOS BIOMÉTRICOS DE IDENTIFICACIÓN** que los elementos mismo de identificación y la información contra cual se confrontan los datos es intransferible.
- Otra técnica de autenticación utiliza el **reconocimiento facial**, por medio de los caracteres almacenados en las bases de datos relacionados al programa de reconocimiento, verificaran las características y en cuestión de segundos aceptará o rechazará la solicitud.

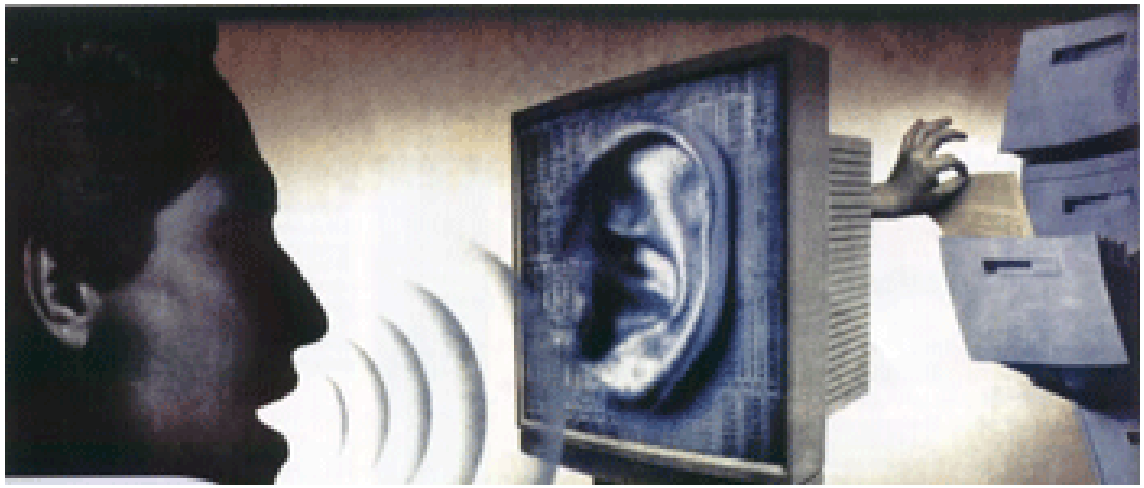
Identificación biométrica



Identificación biométrica

- La forma de **reconocimiento biométrico basado en la voz**, con ciertos caracteres prefijados y con ciertas palabras claves se complementa el método para tener acceso y de esta manera la voz del usuario es comparada con un registro anterior del sistema.

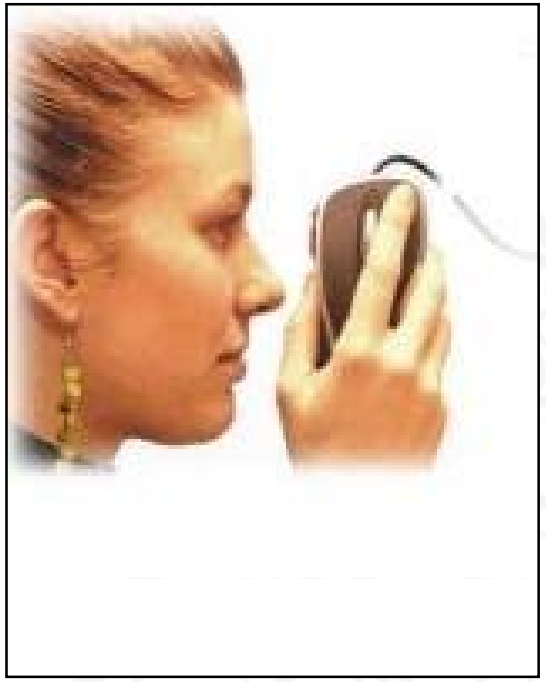
Identificación biométrica



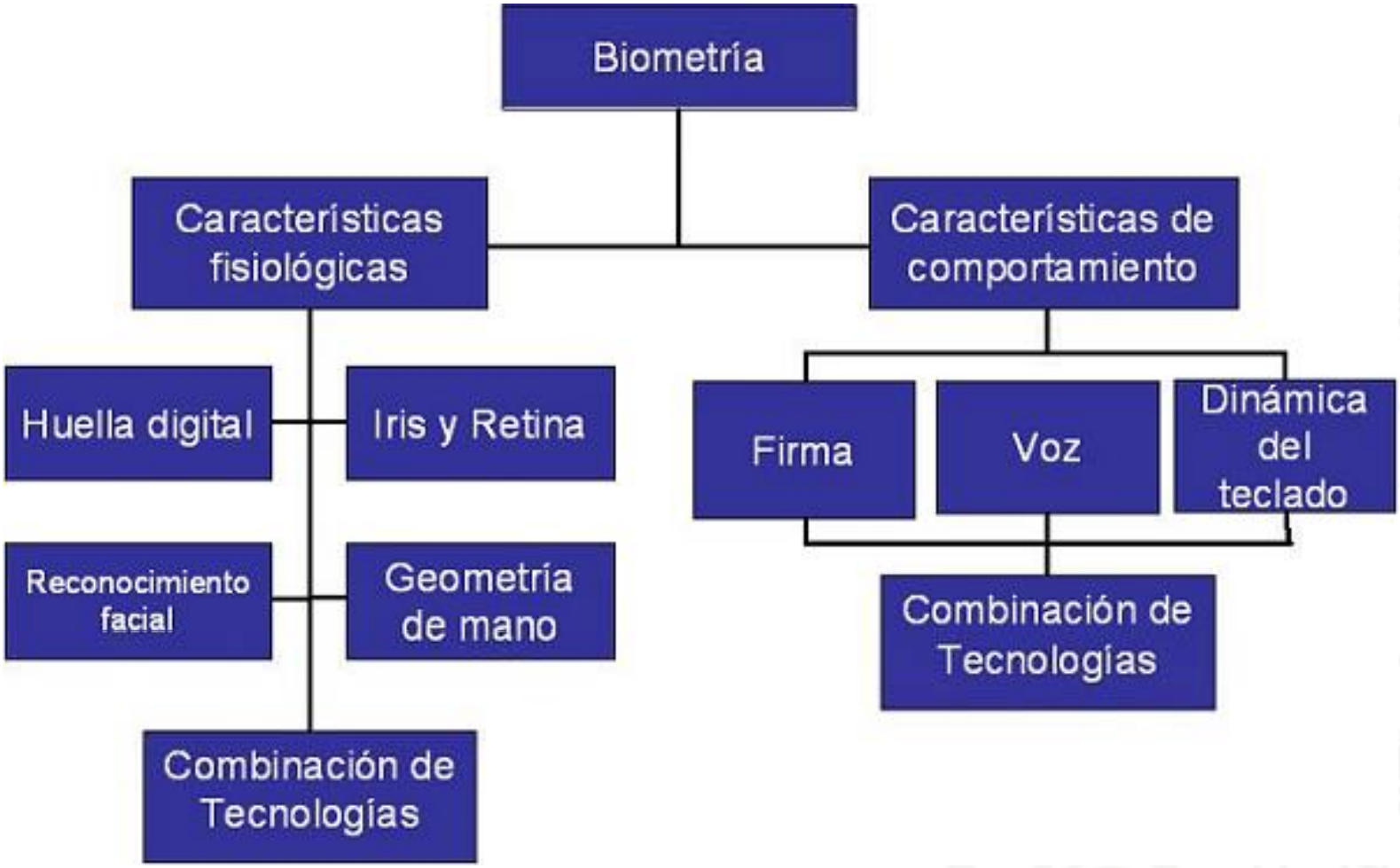
Identificación biométrica

- El patrón de **reconocimiento a través del iris** conforma el método más avanzado de identificación de personas, así como las demás formas, los métodos biométricos llegan a tener un 98% de efectividad.

Identificación biométrica



Identificación biométrica



Identificación biométrica

Identificación biométrica

- La **BIOMETRÍA** tiene el potencial de utilizarse en cualquier aplicación donde la autenticación, verificación e identificación se precisen y sólo es una cuestión de tiempo el poderlos encontrar y usar en nuestras vidas diarias (hogar, trabajo, transportes, diversión, acceso a cuestiones municipales, sociales, de gobierno, sanitarias, etc.).

Caracterización de la biometría

- La **BIOMETRÍA** puede definirse de diferentes formas: **(1)** Según el **ISO** es una característica física o un rasgo de comportamiento de una persona medible utilizado para reconocer la identidad o verificar la identidad declarada de una persona inscrita.

Caracterización de la biometría

- Así mismo, según el **ISO** un **SISTEMA BIOMÉTRICO** es un sistema automatizado capaz de: (i) Capturar una muestra biométrica de un usuario final. (ii) Extraer datos biométricos de dicha muestra. (iii) Comparar los datos biométricos con los contenidos en una o varias plantillas de referencia. (iv) Decidir como de bien coinciden. (v) Indicar si ha sido realizada o no una identificación o verificación de la identidad.

Caracterización de la biometría

- **(2)** Es una tecnología que verifica la identidad de una persona utilizando información biométrica concreta del individuo como distribución de venas de la palma, huellas dactilares, venas del dedo (o FV, Finger Vein), rasgos faciales, patrón de la oreja, firma manuscrita o trazas biológicas como DNA en sangre o saliva.

Caracterización de la biometría

- **(3)** Es una tecnología que confirma la identidad de una persona comparando en tiempo real los patrones de características físicas/fisiológicas/biológicas/ y de comportamiento de la persona con registros/plantillas/modelos de computador inscritos relativos a dichos patrones.

Caracterización de la biometría

- **(4)** Es una tecnología que utiliza características físicas o de comportamiento de un individuo que pueden medirse y que se comparan para verificar o identificar de forma precisa a un individuo.
- **(5)** Es el estudio de los métodos para el reconocimiento, de forma única, de las personas en base a uno o más rasgos físicos o de comportamiento intrínsecos.

Caracterización de la biometría

- **(6)** Es la identificación de seres vivos basada en características fisiológicas y/o de comportamiento.
- **(7)** Es el uso automatizado de características fisiológicas o de comportamiento para determinar o verificar una identidad.

Sistemas de Control de Acceso

- Las políticas de acceso más comunes en el área de la informática son: **MANDATORY ACCESS CONTROL** (**MAC**) y **DISCRETIONARY ACCESS CONTROL** (**DAC**).
- **DISCRETIONARY ACCESS CONTROL** es una forma de acceso a recursos basada en los propietarios y grupos a los que pertenece un objeto.

Sistemas de Control de Acceso

- Se dice que es **DISCRECIONAL** en el sentido de que un sujeto puede transmitir sus permisos a otro sujeto.
- La mayoría de los sistemas Linux usan este tipo de acceso, estando los permisos orquestados por grupos y usuarios, pudiendo un usuario normal cambiar los permisos de los archivos que posee con el comando **chmod**.

Sistemas de Control de Acceso

- **MANDATORY ACCESS CONTROL** en cambio se basa en políticas.
- Existen un conjunto de reglas de autorización (políticas) las cuales determinan si una operación sobre un objeto realizada por un sujeto está o no permitida basándose en los atributos de ambos.

Sistemas de Control de Acceso

- En este caso, el **MANDATORY** refleja el hecho de que las políticas están centralizadas y no pueden ser sobrescritas por un sujeto.
- La diferencia, una vez descritas las dos políticas, salta a la vista. En **DAC** el acceso está descentralizado, siendo el propietario de cada objeto el encargado de asignar los permisos de los diversos sujetos (grupos en el caso de Unix/Linux) que accederán a ellas.

Sistemas de Control de Acceso

- En cambio con el **MAC** los objetos y los sujetos tan solo tienen atributos, pero son las políticas las que se encargan de autorizar o denegar una acción.
- Como se ha comentado, en los entornos GNU/Linux lo habitual suele ser el sistema de control de acceso **DAC**, pero hay excepciones.

Sistemas de Control de Acceso

- **Red Hat** ha apostado fuerte por **SELinux** a partir de un desarrollo de la NSA en Diciembre del 2000 que fue aceptado dentro del kernel 2.6.0-test3, liberado en agosto del 2003, e implementado por primera vez dentro de RHEL 4.

Sistemas de Control de Acceso

- También **Suse Linux** quiso implementar un sistema **MAC**, y lo hizo a través de **AppArmor**, cuyo equipo de desarrollo mantuvo hasta el 2007. Su primera inclusión por defecto en **Suse** fue en **SuSe Linux Enterpise Server 10**.

Resumen

- Existen varios sistemas para verificar la identidad de un individuo, sin embargo la **biometría** se considera como el método más apropiado, ya que ciertos rasgos de cada persona, son inherentes a ella y sólo a ella.
- La **biometría** permite una autentificación segura, al contrario que el empleo de contraseñas o tarjetas, ya que estos últimos pueden ser robados o utilizados por personas no autorizadas.