**AUTENTIFICACION O AUTENTICACIÓN**

**Autentificacion o Autenticación** es el acto de establecimiento o confirmación de algo (o alguien) como auténtico. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores.

**Definiciones**

**Autenticación**, **autentificación** (no recomendado) o mejor dicho acreditación, en términos de [seguridad](http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica) de [redes](http://es.wikipedia.org/wiki/Red_de_computadoras) de [datos](http://es.wikipedia.org/wiki/Datos), se puede considerar uno de los tres pasos fundamentales ([AAA](http://es.wikipedia.org/wiki/Protocolo_AAA)). Cada uno de ellos es, de forma ordenada:

1. **Autenticación**. En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quien ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.
2. [**Autorización**](http://es.wikipedia.org/wiki/Autorizaci%C3%B3n)**.** Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
3. [**Auditoría**](http://es.wikipedia.org/wiki/Auditor%C3%ADa)**.** Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

El problema de la autorización a menudo, es idéntico a la de autenticación; muchos protocolos de seguridad extensamente adoptados estándar, regulaciones obligatorias, y hasta estatutos están basados en esta asunción. Sin embargo, el uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación que una persona conocida tiene la autoridad para realizar una cierta operación. La autenticación, por lo tanto, debe preceder la autorización. Para distinguir la autenticación de la autorización de término estrechamente relacionada.

**Métodos de autenticación**

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

* Sistemas basados en algo conocido. Ejemplo, un *password*  ([Unix](http://es.wikipedia.org/wiki/Unix)) o *passphrase* ([PGP](http://es.wikipedia.org/wiki/Pretty_Good_Privacy)).
* Sistemas basados en algo poseído. Ejemplo, una tarjeta de identidad, una [tarjeta inteligente](http://es.wikipedia.org/wiki/Tarjeta_inteligente)(*smartcard*), dispositivo usb tipo epass token, smartcard o [dongle criptográfico](http://es.wikipedia.org/wiki/Mochila_%28dispositivo%29%22%20%5Co%20%22Mochila%20%28dispositivo%29).
* Sistemas basados en una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares.

**Características de autenticación**

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).

Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).

Soportar con éxito cierto tipo de ataques.

Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

**Mecanismo general de autenticación**

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de [autorización](http://es.wikipedia.org/wiki/Autorizaci%C3%B3n) y/o [auditoría](http://es.wikipedia.org/wiki/Auditor%C3%ADa) oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único (valga la redundancia). Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como login.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

**Control de acceso**

Un ejemplo familiar es el control de acceso. Un sistema informático supuesto para ser utilizado solamente por aquellos autorizados, debe procurar detectar y excluir el desautorizado. El acceso a él por lo tanto es controlado generalmente insistiendo en un procedimiento de la autentificación para establecer con un cierto grado establecido de confianza la identidad del usuario, por lo tanto concediendo esos privilegios como puede ser autorizado a esa identidad. Los ejemplos comunes del control de acceso que implican la autenticación incluyen:

* Retirar de dinero de un cajero automático.
* Control de un computador remoto sin Internet.
* Uso de un sistema Internet banking.

Sin embargo, observar que mucha de la discusión sobre estos asuntos es engañosa porque los términos se utilizan sin la precisión. Parte de esta confusión puede ser debido “al tono de la aplicación de ley” de mucha de la discusión. Ninguna computadora, programa de computadora, o poder del usuario de la computadora “confirman la identidad” de otro partido. No es posible “establece” o “probar” una identidad, cualquiera. Hay ediciones difíciles que están al acecho debajo de qué aparece ser una superficie directa.

Es solamente posible aplicar una o más pruebas que, si están pasadas, se han declarado previamente para ser suficientes proceder. El problema es determinarse qué pruebas son suficientes, y muchos tales son inadecuadas.

Tienen sido muchos casos de tales pruebas que son spoofed con éxito; tienen por su falta demostrada, ineludible, ser inadecuadas. Mucha gente continúa mirando las pruebas -- y la decisión para mirar éxito en pasar -como aceptable, y para culpar su falta en “sloppiness” o “incompetencia” de parte alguien.

 El problema es que la prueba fue supuesta para trabajar en la práctica -- no bajo condiciones ideales de ningún sloppiness o incompetencia-y no. Es la prueba que ha fallado en tales casos. Considerar la caja muy común de un email de la confirmación a el cual deba ser contestado para activar una cuenta en línea de una cierta clase. Puesto que el email se puede arreglar fácilmente para ir a o para venir de direcciones falsas y untraceable, éste es justo sobre la menos autenticación robusta posible. El éxito en pasar esta prueba significa poco, sin consideración alguna hacia sloppiness o incompetencia.

**Autenticación por multifactor**

Los factores de la autenticación para los seres humanos se clasifican, generalmente, en cuatro casos:

* Algo que el usuario es (ejemplo, la huella digital o el patrón retiniano), la secuencia de ADN (hay definiciones clasificadas de cuál es suficiente), el patrón de la voz (otra vez varias definiciones), el reconocimiento de la firma, las señales bio-eléctricas únicas producidas por el cuerpo vivo, u otro identificador biométrico).
* Algo que el usuario tiene (ejemplo, tarjeta de la identificación, símbolo de la seguridad, símbolo del software o teléfono celular)
* Algo que el usuario sabe (ejemplo, una contraseña, una frase o un número de identificación personal (el PIN) del paso).
* Algo que el usuario hace (ejemplo, reconocimiento de voz, firma, o el paso).
* Autenticación mediante dos factores "algo que tengo" la llave + "algo que sé" un número de PIN (token criptográfico)
* Autenticación triple factor "algo que tengo" el dispositivo criptográfico + "algo que sé" una clave de autenticación tipo PIN (al token criptográfico) + "quién soy" la huella dactilar que me permite autenticarme al dispositivo de forma unívoca.

Una combinación de métodos se utiliza a veces, ejemplo, una tarjeta de banco y un PIN, en este caso se utiliza el término “autenticación de dos factores”. Históricamente, las huellas digitales se han utilizado como el método más autoritario de autenticación, pero procesos legales recientes en los E.E.U.U. y a otra parte han levantado dudas fundamentales sobre fiabilidad de la huella digital. Otros métodos biométricos son prometedores (las exploraciones retinianas y de la huella digital son un ejemplo), pero han demostrado ser fácilmente engañados en la práctica. En un contexto de los datos de la computadora, se han desarrollado [protocolos de desafío-respuesta](http://es.wikipedia.org/wiki/Protocolos_desaf%C3%ADo-respuesta) que permiten el acceso si el que se quiere autenticar responde correctamente a un desafío propuesto por el verificador. Hay [protocolos desafío-respuesta](http://es.wikipedia.org/wiki/Protocolos_desaf%C3%ADo-respuesta) basados en algoritmos criptográficos llamándose [protocolos criptográficos de desafío-respuesta](http://es.wikipedia.org/wiki/Protocolos_desaf%C3%ADo-respuesta). La seguridad de los [protocolos criptográficos de desafío-respuesta](http://es.wikipedia.org/wiki/Protocolos_desaf%C3%ADo-respuesta) se basa en la seguridad de los [algoritmos criptográficos](http://es.wikipedia.org/wiki/Criptograf%C3%ADa) que usa.

**Autenticación clásica**

En un sistema Unix habitual cada usuario posee un nombre de entrada al sistema o login y una clave o password; ambos datos se almacenan generalmente en el fichero /etc/passwd. Este archivo contiene una línea por usuario donde se indica la información necesaria para que los usuarios puedan conectar al sistema y trabajar en él, separando los diferentes campos mediante `:'.

Al contrario de lo que mucha gente cree, Unix no es capaz de distinguir a sus usuarios por su nombre de entrada al sistema. Para el sistema operativo lo que realmente distingue a una persona de otra (o al menos a un usuario de otro) es el UID del usuario en cuestión; el login es algo que se utiliza principalmente para comodidad de las personas (obviamente es más fácil acordarse de un nombre de entrada como *toni* que de un UID como *2643*, sobre todo si se tienen cuentas en varias máquinas, cada una con un UID diferente).

Para cifrar las claves de acceso de sus usuarios, el sistema operativo Unix emplea un criptosistema irreversible que utiliza la función estándar de C crypt, basada en el algoritmo DES. Para una descripción exhaustiva del funcionamiento de crypt. Esta función toma como clave los ocho primeros caracteres de la contraseña elegida por el usuario (si la longitud de ésta es menor, se completa con ceros) para cifrar un bloque de texto en claro de 64 bits puestos a cero; para evitar que dos passwords iguales resulten en un mismo texto cifrado, se realiza una permutación durante el proceso de cifrado elegida de forma automática y aleatoria para cada usuario, basada en un campo formado por un número de 12 bits (con lo que conseguimos 4096 permutaciones diferentes) llamado salt. El cifrado resultante se vuelve a cifrar utilizando la contraseña del usuario de nuevo como clave, y permutando con el mismo salt, repitiéndose el proceso 25 veces. El bloque cifrado final, de 64 bits, se concatena con dos bits cero, obteniendo 66 bits que se hacen representables en 11 caracteres de 6 bits cada uno y que, junto con el salt, pasan a constituir el campo password del fichero de contraseñas, usualmente /etc/passwd. Así, los dos primeros caracteres de este campo estarán constituidos por el salt y los 11 restantes por la contraseña cifrada

**Problemas del modelo clásico**

Los ataques de texto cifrado escogido constituyen la principal amenaza al sistema de autenticación de Unix; a diferencia de lo que mucha gente cree, no es posible descifrar una contraseña, pero es muy fácil cifrar una palabra junto a un determinado salt, y comparar el resultado con la cadena almacenada en el fichero de claves. De esta forma, un atacante leerá el fichero /etc/passwd (este fichero ha de tener permiso de lectura para todos los usuarios si queremos que el sistema funcione correctamente), y mediante un programa adivinador (o crackeador) cifrará todas las palabras de un fichero denominado diccionario (un fichero [ASCII](http://es.wikipedia.org/wiki/ASCII) con un gran número de palabras de cualquier idioma o campo de la sociedad: historia clásica, deporte, cantantes...), comparando el resultado obtenido en este proceso con la clave cifrada del fichero de contraseñas; si ambos coinciden, ya ha obtenido una clave para acceder al sistema de forma no autorizada.

**Shadow Password**[[editar](http://es.wikipedia.org/w/index.php?title=Autenticaci%C3%B3n&action=edit&section=11)]

Otro método cada día más utilizado para proteger las contraseñas de los usuarios el denominado Shadow Password u oscurecimiento de contraseñas. La idea básica de este mecanismo es impedir que los usuarios sin privilegios puedan leer el fichero donde se almacenan las claves cifradas.

**Envejecimiento de contraseñas**

En casi todas las implementaciones de Shadow Password actuales se suele incluir la implementación para otro mecanismo de protección de las claves denominado envejecimiento de contraseñas (Password Aging). La idea básica de este mecanismo es proteger los passwords de los usuarios dándoles un determinado periodo de vida: una contraseña sólo va a ser válida durante un cierto tiempo, pasado el cual expirará y el usuario deberá cambiarla.

Realmente, el envejecimiento previene más que problemas con las claves problemas con la transmisión de éstas por la red: cuando conectamos mediante mecanismos como[telnet](http://es.wikipedia.org/wiki/Telnet), [ftp](http://es.wikipedia.org/wiki/Ftp) o rlogin a un sistema Unix, cualquier equipo entre el nuestro y el servidor puede leer los paquetes que enviamos por la red, incluyendo aquellos que contienen nuestro nombre de usuario y nuestra contraseña.

**CAJEROS VIRTUALES**

La mayoría de los bancos y cajas de ahorro de todos los países ofrecen ya servicios de banca electrónica, incluyendo servicios y contratos TPVV (Terminal Punto de Venta Virtual), lo que se llama, a veces, cajeros virtuales.

Los contratos TPV (Terminal Punto de Venta) son los contratos normales que se establecen entre un comerciante y la entidad financiera con la que trabaje habitualmente para poder aceptar el pago con tarjeta de los clientes.  Todos los usuarios de tarjetas conocemos este sistema. El comerciante dispone de una pequeña máquina, comunicada con la pasarela de pago por vía telefónica, por la que pasa la banda magnética de nuestra tarjeta y recibe la autorización para la venta tras comprobarse la validez de la tarjeta y la disponibilidad de fondos asociados a la misma.

El TPV Virtual es el sistema más seguro para la utilización de las tarjetas de crédito en Internet. Este sistema no solo garantiza que los datos de la tarjeta viajarán, encriptados, directamente del comprador al banco intermediario sino que además, no serán conocidos en ningún momento por el vendedor. Las entidades bancarias son siempre más fiables en la protección de los datos de sus clientes. El sistema es igualmente transparente y ágil para el comprador.

|  |
| --- |
|  |

 El vendedor, la tienda virtual, necesita tener un contrato TPV con su banco habitual que le permita el cobro con tarjeta de crédito. El TPV Virtual es un contrato específico que permite cobrarse de tarjetas de crédito a través de Internet. Cuando se establece este contrato entre el vendedor y su banco, el banco proporciona un paquete de programas para ser instalados en el servidor que aloja la tienda virtual.



La tienda virtual ofrece en páginas web el catálogo de sus productos y un formulario de pedido. El formulario puede tener la forma de carro de compra virtual

 1.- El comprador visita las páginas web de la tienda virtual. Va seleccionando los productos que desea y añadiéndolos al carro de compra virtual. Una vez que concluye su compra, inicia el proceso de pago pulsando el botón correspondiente.

 2.- El paquete de programas CGI proporcionados por el banco e incorporados a la tienda virtual realiza las siguientes operaciones:
 a)     Genera un identificador que es específico de esa transacción.
b)     Archiva para el vendedor los datos del pedido: la lista de productos y la forma y dirección para el envío, junto con el identificador.
c)     Envía al banco los datos esenciales de la transacción: la identidad del vendedor, el identificador de la transacción y su importe.

3.- En la pantalla del comprador aparece un formulario web que ya no está alojado en el servidor del vendedor sino en el del banco, que es un servidor con seguridad tipo SHTTP o SSL. En ese formulario consta el importe total de la operación y se identifica al vendedor. El comprador introduce en el formulario del banco los datos de su tarjeta de crédito. Los datos viajan encriptados al banco.

 4.- El banco comprueba la validez de la tarjeta. Una vez comprobado, realiza los cargos y abonos correspondientes y comunica al vendedor que la transacción correspondiente al identificador es válida.

 5.- El vendedor procede al envío de la compra.

 Con respecto al sistema básico, el TPV Virtual ofrece más seguridad ya que los datos de la tarjeta de crédito del comprador son transmitidos directamente al banco. Las entidades bancarias son bien conocidas por los usuarios de Internet e inspiran más confianza que una tienda virtual desconocida. Con este sistema el intermediario bancario no sólo está facilitando la transacción sino que además está ofreciendo su propia garantía para confianza del comprador.