TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1-UNIDAD 3

TIC

Universidad Tecnológica de Pereira

faceIT

Autenticación y autorización

La ciberseguridad depende de varios factores para que los datos estén protegidos y se tenga confianza en que los sistemas codifican y protegen los datos como se ha planeado. Un factor que permite garantizar la seguridad sobre los datos es la autenticación, que es un mecanismo para determinar que una persona que intenta acceder a ciertos datos es quien dice ser. Para que la autenticación funcione debe ser sencilla para el usuario y tener solidez en cuanto a la seguridad informática.

La autenticación concede a cada usuario un nivel específico de acceso a los datos y a los recursos. Según el acceso que cada usuario necesita para sus labores, existirán roles sobre el sistema y restricciones dependiendo del rol. Como ejemplo podemos suponer la administración de un hotel. En el hotel una persona que haya registrado una reserva, al llegar debe mostrar su identificación. Con esta identificación se valida que es quien dice ser y se le entrega una llave que le permite el acceso a su habitación y a las zonas para los huéspedes (restaurante, gimnasio, piscina, entre otros). La llave de acceso es igual a la autorización ya que le permite acceder a su habitación. El acceso a las zonas de interés para los huéspedes es igual a la autorización, es decir, la autorización determina a donde puede ir y qué puede ver.

Métodos de autenticación:

Usualmente, al comprar con una tarjeta de crédito, se suele solicitar un documento para validar que el portador de la tarjeta es el dueño. De esta forma, quien realizará el cargo a la tarjeta, puede validar que la persona que intenta pagar es quien dice ser. En este ejemplo, la identificación ayuda a verificar la identidad.

De la misma forma, si se quiere acceder a un equipo o a un dispositivo, se necesita un mecanismo de autenticación. Generalmente se emplea un nombre de usuario y una contraseña. El nombre de usuario indica quien es y la contraseña ayuda a validar que el usuario es quien dice ser. Sin embargo, el hecho de que un usuario sea autenticado en un sistema, la autenticación no rige lo que puede hacer cuando se haya autenticado. Ese mecanismo que controla lo que un usuario puede hacer es la autorización.

Existen diferentes formas para autenticar a un usuario de forma segura, como siempre, intentando validar que es quien dice ser. Para eso se pueden usar tres tipos de datos. Datos que el usuario sabe, objetos que el usuario tiene e información que forma parte del usuario.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

Respecto a los datos que el usuario sabe se tiene:

- Contraseñas
- Números de pin
- Preguntas de seguridad

Objetos que el usuario tiene:

- Documentos de identidad
- Llaves USB
- Computadores
- Teléfonos móviles

Información que hace parte del usuario:

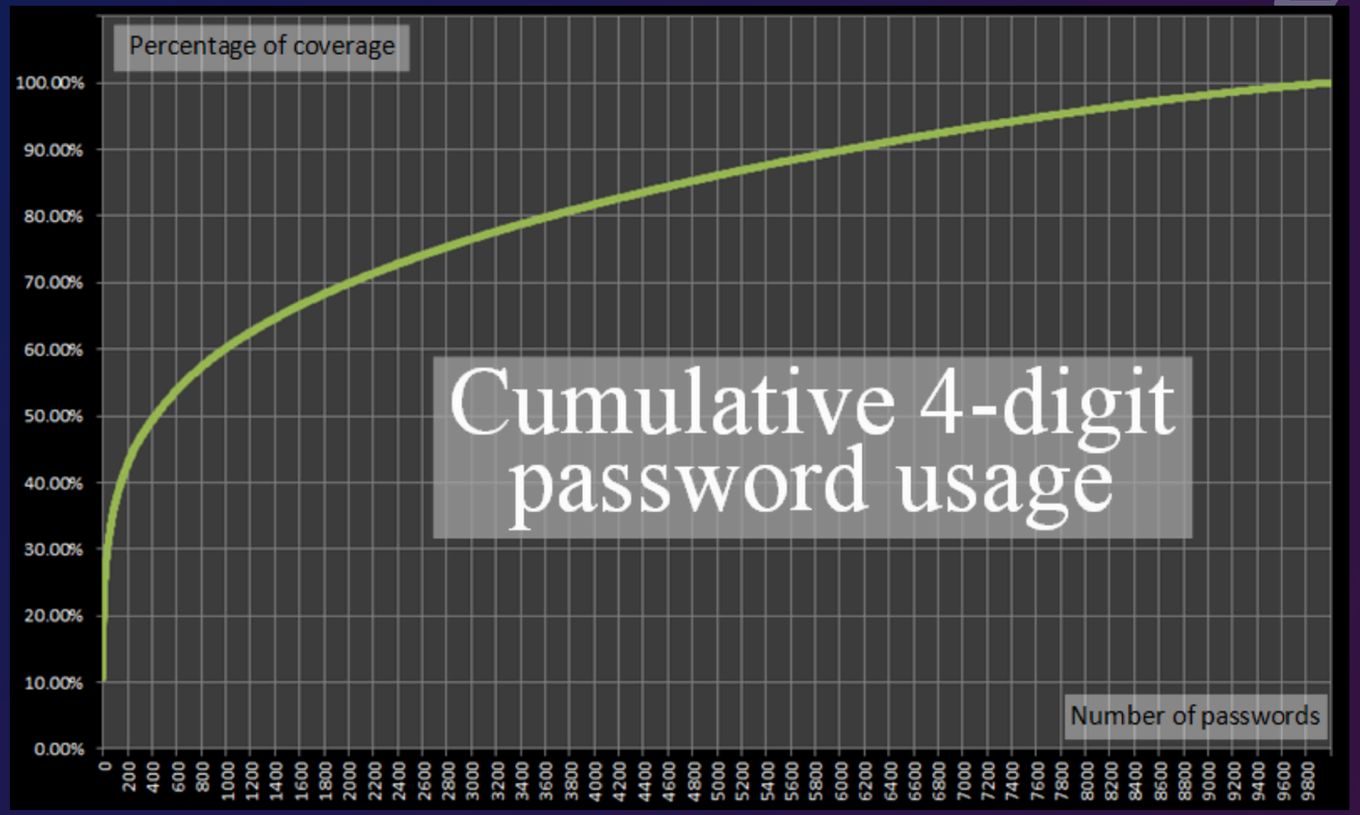
- Una huella digital
- Reconocimiento facial
- Análisis de la forma y color de su retina
- Cualquier forma de identificación biométrica

Autenticación de un factor (o factor único)

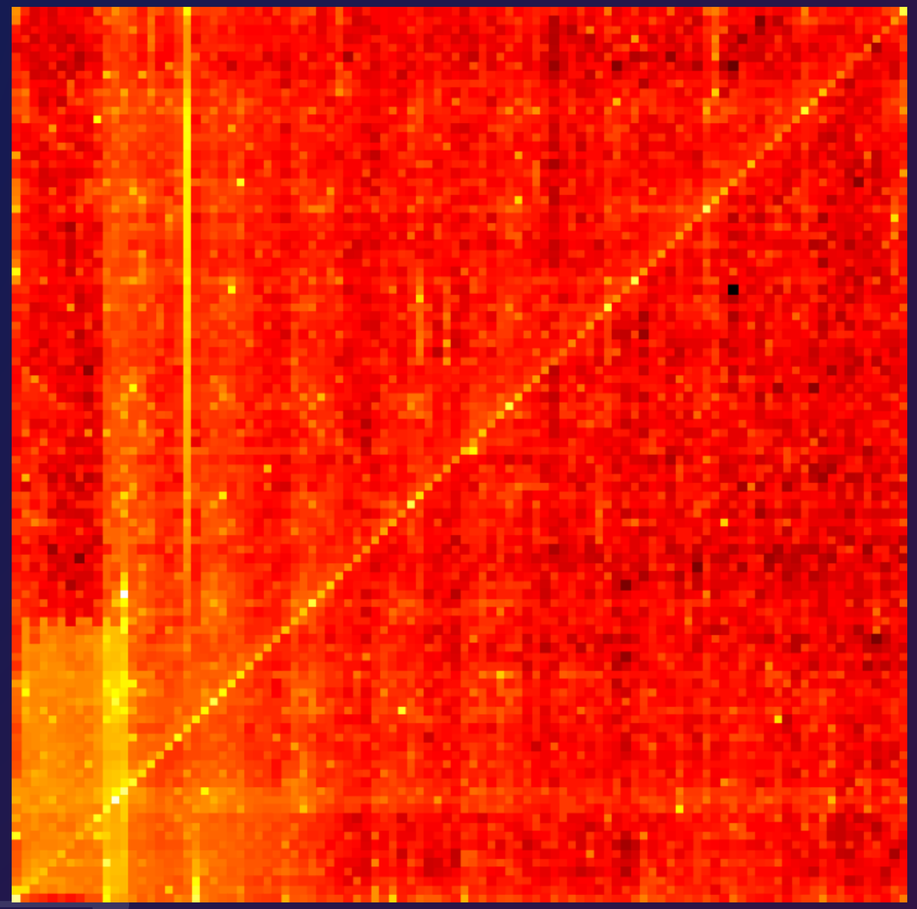
Es un sistema que usa solo un tipo de autenticación, por tal motivo es un método menos seguro, pero es el más sencillo. Tengamos en cuenta que siempre habrá un intercambio entre la sencillez del método de autenticación para el usuario y la seguridad que proporciona.

Un ejemplo de un factor único de autenticación es solicitando al usuario algo que sabe. Por ejemplo, una contraseña.

El problema de las contraseñas es que las más simples y fáciles de recordar, también son fáciles de piratear. Por ejemplo, las claves de las tarjetas de banco que usan 4 dígitos numéricos. Con 4 dígitos existen 10.000 posibilidades, pero en general se usan muchas menos combinaciones. Existen varios conjuntos de datos con contraseñas filtradas en brechas de seguridad. Al analizar estos datos (3.4 millones de registros) los estudios mostraron que cerca del 11% de las claves era 1234.Seguido por 1111 con el 6% de repeticiones sobre la base de datos. Es decir, si las combinaciones fuesen aleatorias, se esperaría que ningún número supere el 0.2% de probabilidad de ser escogido, sin embargo, las contraseñas más fáciles de recordar se usan más a menudo.



Si se analiza la frecuencia acumulativa de probabilidad. Un tercio de las combinaciones puede ser adivinada solamente probando 61 combinaciones.



Mapa de calor de las combinaciones

Si se revisan los datos como un mapa de calor, se aprecia que las combinaciones más probables (tienden a blanco) están situadas en los números 0000, 1111, 2222, 3333, 4444, 5555, 6666 y así sucesivamente. También se aprecia que la gente suele emplear el año de nacimiento o fechas para definir sus claves, por lo que la parte inferior del gráfico que tiene los dígitos 19xx o dígitos relativos a los meses y días del año suelen aparecer con mucha mayor frecuencia.

Igualmente, las palabras sencillas de menos de 6 letras se pueden adivinar con ensayo y error en menos de 1 segundo. Por lo que un atacante con un diccionario de datos asociados a un usuario podría adivinar fácilmente las contraseñas más sencillas.

La firma de ciberseguridad Hive Systems ha producido un gráfico de los tiempos estimados para adivinar una contraseña, se puede ver que una contraseña de 7 caracteres se puede adivinar por ensayo y error en tan solo dos segundos, incluso si la clave tiene números, mayúsculas y minúsculas. Si la contraseña tiene solamente números, se puede romper en menos de un segundo con hasta 12 dígitos.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Tabla con los tiempos que tarda una contraseña en ser vulnerada dependiendo del número de caracteres.

Otro método de autenticación de un factor que evita el recordar contraseñas es empleando un objeto que el usuario posea. Por ejemplo, si el usuario quiere pagar con su tarjeta de crédito, al pagar debe generar una clave variable que se valida en el teléfono móvil.
También se puede utilizar alguna forma biométrica para validar la identidad, como, por ejemplo, solicitar al usuario que use la huella digital para desbloquear un teléfono móvil o para realizar un pago.
Si bien la autenticación con un factor es fácil para el usuario, no es apropiada para que un sistema sea seguro.

Múltiple factor de autenticación

La autenticación multifactor es un sistema en el que se usan dos o incluso tres tipos de autenticación. Al proporcionar algo que sabe, algo que tiene y algo que forma parte de del usuario, se incrementa considerablemente la seguridad en un sistema.
Es usual que en cuentas bancarias se pida una contraseña y una clave que se envía a su teléfono móvil para realizar una transacción. Esto es, un dato que el usuario sabe y algo que el usuario tiene. También es posible que se validen mediciones biométricas, gracias a los sensores integrados en el celular.
Este método es más seguro, sin embargo, requiere que el usuario dé más pasos para autenticarse.