Configuración de sistemas de control de acceso y autenticación de personas.

Caso práctico

Direct Media (CC0)

El CEO de la clínica se ha dado cuenta de la importancia que tiene garantizar el proceso de conexión a los sistemas y aplicaciones. La creación de una fuente única y fiable de las identidades, asociada a la gestión de los derechos son los dos pilares de una buena infraestructura de gestión de las identidades y accesos.

Por tanto, se ha planteado identificar los principales mecanismos de autenticación para que los sistemas de información de la clínica garanticen la correcta identidad de los usuarios y les asocie correctamente sus derechos.

Objetivos:

En esta unidad el alumno podrá descubrir las diferencias entre los distintos mecanismos de autenticación para el acceso a los servicios y sistemas, así como los principios básicos acerca de:

- Identificación
- Autenticación
- Autorización

Se analizarán además, los tipos de factor relativos al doble factor de autenticación y al multifactor.

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Ministerio de Educación y Formación Profesional (Dominio público)

1.- Mecanismos de autenticación.

Caso práctico

u_h0yvbj97 (Dominio público)

Los mecanismos de autenticación son esenciales. Imaginemos que necesitamos acceder de manera exclusiva a un sitio de manera física. Si ese lugar no es protegido mediante alguna medida, como una cerradura con llave o similar, cualquiera podría entrar. Esto mismo se aplica al mundo lógico donde se han de proteger los accesos mediante tecnologías.

A lo largo de esta unidad iremos analizando los distintos mecanismos de autenticación existente para el acceso a los servicios, tecnologías, etc. Es de sobra conocido que, desde tiempo inmemorial, las personas han protegido sus posesiones, artículos de valor, riquezas, etc. con algún tipo de mecanismo o elemento que impidiera el acceso a personas ajenas a la propiedad. Pudo ser un elemento pesado como una roca hace decenas de miles de años, las primeras cerraduras que se crearon en el antiguo Egipto, las cajas fuertes durante la fiebre del oro americana, o a la dupla de usuario y contraseña usados de manera conjunta hasta hace unos años. Todos ellos, se pueden considerar “controles de acceso”.

Pero ¿qué es un control de acceso? Podríamos contestar a esta pregunta desarrollando alguno de los ejemplos vistos anteriormente, pero podríamos clasificarlos en dos grupos. Por un lado, los controles de acceso físico, como puertas, cajas fuertes, etc. y los controles de acceso lógicos, como el usuario y contraseña que nos da acceso a un servicio. No obstante, también podemos hablar de controles de acceso mixtos, como por ejemplo la puerta que, para ser abierta, necesita que introduzcamos una contraseña o acerquemos algún tipo de token o tarjeta RFID.

Y ¿Qué tienen que ver los controles de acceso con los mecanismos de autenticación? Pues mucho, pero antes necesitamos conocer cuáles son los principios básicos que se establecen para un control de acceso.

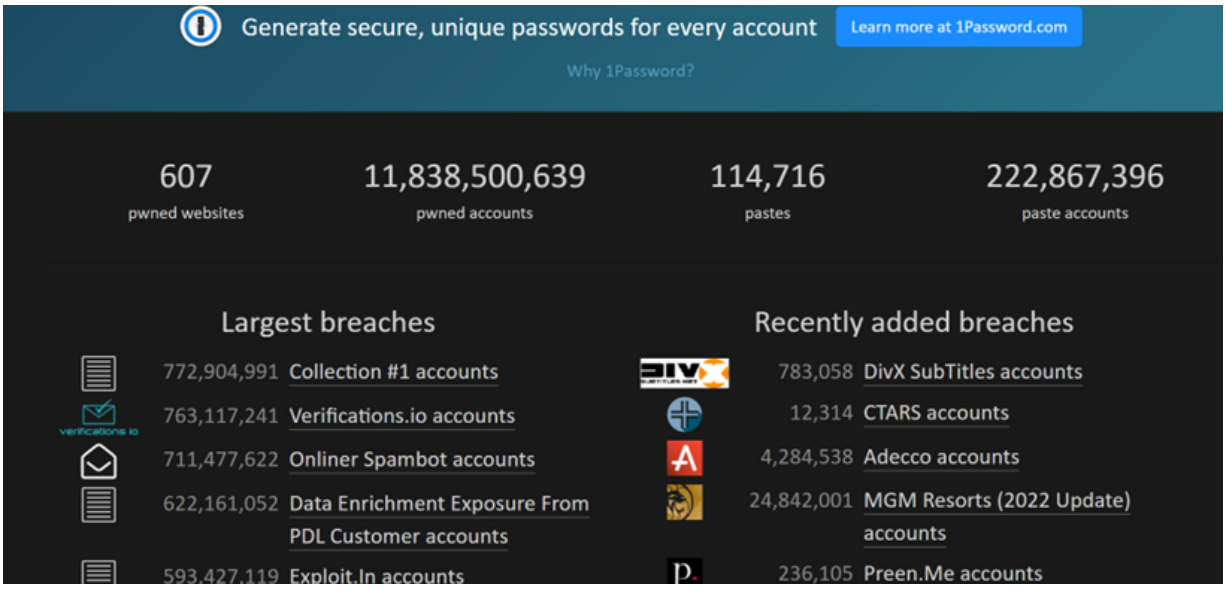
1.1.- Principios básicos para el control de acceso.

A continuación se describen los tres principios básicos

Identificación

Se trata del proceso inicial necesario para acceder a un lugar de manera física o a un recurso de manera lógica. En este punto entran en juego diversos mecanismos que pueden utilizarse para llevar a cabo el proceso entre los que destacan:

Usuario/contraseña: sin duda uno de los mecanismos más utilizados hasta la actualidad, pero que hoy en día no es suficiente ya que los atacantes han sofisticado la posibilidad de engañar a los usuarios a través de suplantaciones (phishing) y también, por la gran cantidad de brechas de seguridad que han dejado expuestos millones de credenciales. Solo hace falta pasar el por el servicio “Have I been Powned" para ver la cantidad de información que han recopilado:



https://haveibeenpwned.com/ (Dominio público)

Biometría: si en el anterior punto utilizamos una información que “sabíamos”, en este caso el elemento para identificarnos será algo que “somos”. En este sentido y dejando a un lado todas las cuestiones legales en torno a la privacidad por el almacenamiento de características físicas, se trata de un mecanismo que a pesar de ser considerado como “infalible” lo cierto es que aún tiene recorrido para ser preciso. Algunos elementos físicos, utilizados en la biometría son desde la huella dactilar, hasta expresiones faciales específicas pasando por la voz y el iris.

Tokens, tarjetas físicas y otros dispositivos: se trata de algo que "tenemos". Normalmente son utilizadas más para el acceso físico que el acceso lógico, pero no debemos olvidar que también existen tarjetas que llevan un chip integrado con un certificado y que son usadas para, por ejemplo, acceder a un sistema informático. También existen sistemas que utilizan los dispositivos móviles como elementos de identificación o para reforzar la seguridad. Pero es algo que veremos más adelante.

Autenticación

Se trata del proceso que sigue a la identificación por el cual, se comprueba en la base de datos o el sistema que permite el acceso, si la información facilitada (contraseña, rasgos biométricos, etc.) coincide con la de algún usuario. En caso afirmativo, el sistema facilita el siguiente paso para el acceso. Pero no es el último paso.

Autorización

Una vez completado todo lo anterior y realizada la lógica de verificación que cada sistema disponga, se procederá a autorizar el acceso al sistema, servicio, tecnología o instalación física. En este punto, entra también en juego lo que se denomina segmentación de acceso o implementación de roles. Esto permitirá segregar las funciones que un determinado usuario tiene sobre el sistema o sobre el acceso físico. Por ejemplo, un usuario que pertenece al departamento de Jurídico de una empresa no tiene por qué acceder al área de investigación o a zonas restringidas.

En la actualidad, utilizar un único factor como medio de autenticación, puede suponer un riesgo, ya que, en caso de captura o robo de credenciales, sustracción del token o incluso técnicas avanzadas como la inyección o modificación de datos biométricos en bases de datos, supondrán una menor protección frente a atacantes.

Para saber más

Si quieres ampliar información acerca de estas técnicas, no dejes de consultar la guía de "Técnicas Biométricas" del INCIBE.

AUTOEVALUACIÓN

Los principios básicos para el control de acceso son:

- ○ • Algo que sé, algo que soy y algo que se tiene
- ○ • Algo que sabe, algo que soy y algo que se tiene
- ○ • Algo que tengo, algo que soy algo que debo

Correcto. Algo que se: usuario y contraseña; algo que soy como un rasgo biométrico; algo que tengo como un token.

Incorrecto

Incorrecto

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

2.- Tipos de factores.

Caso práctico

mohamed_hassan (Dominio público)

Siempre que usamos una aplicación de banca electrónica, vamos a encontrarnos que para realizar una operación, el banco nos va a solicitar una clave de firma o similar. Esta clave en la que usan las entidades para verificar la autorización de la operación y es un factor de autenticación adicional.

Finalizamos el punto anterior explicando acerca de la necesidad de utilizar más de un elemento o factor en los procesos de control de acceso y autenticación. ¿Por qué razón? Básicamente porque a más elementos usemos, más capas de seguridad estaremos aplicando a la hora de acceder a un servicio.

Por ejemplo, resulta que en una brecha de seguridad de la empresa “linkertin” en la que estaba registrado, mis datos han sido expuestos. Y, además como soy un usuario vago que reutilizo mi contraseña, empleo la misma para mi correo, para mis portales de eCommerce favoritos y un largo etcétera. Si un atacante se hace con esa información y resulta que por mi parte no uso ningún elemento o factor adicional más para acceder a los servicios, estaré ante una situación realmente comprometida. Sin embargo, si he configurado el servicio para que a la hora de acceder solicite alguna otra información, sin duda se lo habré puesto muy difícil a alguien que intente acceder a mi información.

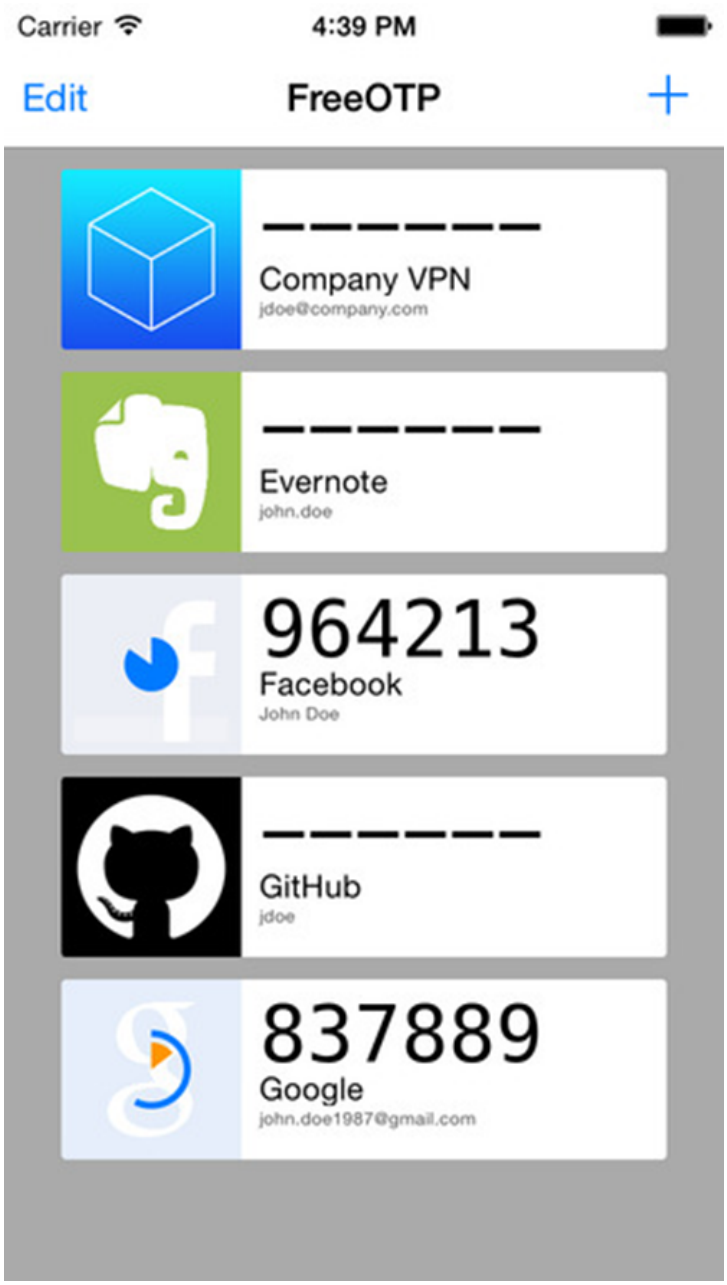
¿Pero qué tipos de autenticación encontramos que usen los distintos factores? Esencialmente dos, el doble factor de autenticación o 2FA, o la autenticación multifactor MFA.

2FA

- Podemos decir que la característica del 2FA, es que esencialmente utiliza uno de los tres factores principales: “algo que sé”, “algo que soy” y “algo que tengo”. En cualquier caso, es posible que un 2FA sea un factor que se repite. Por ejemplo, un servicio que usa el clásico usuario y contraseña y que como 2FA, tiene una contraseña adicional. Este tipo de seguridad va a permitir añadir dos capas de protección a la hora de acceder a un servicio.

  Como dato curioso, es interesante saber que las entidades financieras sujetas a normativa muy rigurosa en lo relativo a la operativa en línea, con la entrada en vigor de la última versión de la PCI DSS, los bancos pasaron de emplear 2FA a MFA ya que esta permite más granularidad en función de las acciones que se lleven a cabo. Por ejemplo, para acceder a la banca online, únicamente necesitaremos el usuario y la contraseña, pero para operar, necesitaremos verificar la operación con una clave y luego firmar con otra. Es por ello que la opción MFA es más segura que el 2FA, no tiene por qué, dependerá de qué necesidades de seguridad tengamos.

  Por último, hay que mencionar que la mayor parte de los servicios de Internet, al menos los más populares, permite la utilización de 2FA a través de diversos métodos como Google Google Autenticator, FreeOTP o incluso vía SMS.



Marco Lozano (Dominio público)

MFA

Tal y como hemos adelantado en el punto previo, la MFA es un tipo de autenticación que permite más de dos factores. Como dejamos claro anteriormente, puede reutilizarse más de un factor para dotar de capas de seguridad a un servicio. ¿Significa que MFA es más seguro?, aunque antes se ha indicado que no necesariamente, es cierto que a mayor número de capas mayor seguridad, pero también influirá en la usabilidad de los usuarios que quizás no se sientan cómodos con tanta “capa”. ¿Qué soluciones tenemos frente a eso? Pues por fortuna, existen iniciativas que consideran más elementos como capas de seguridad. Por ejemplo, la ubicación geográfica, el tipo de terminal, etc. Esto se refleja en tecnologías como:

- MFA adaptativo: donde se tienen en cuenta cuestiones como la ubicación. Como ejemplo, si tenemos habilitado el 2FA o MFA en las cuentas de Google a las que habitualmente accedemos desde España, si nos vamos a USA, cuando intentemos conectarnos, nos preguntará por el 2FA o MFA.
- SSO o inicio de sesión único: lo vemos casi permanentemente en servicios de Internet donde para darnos de alta, ya no es necesario registrarnos si no que podemos vincular la información a una cuenta existente de Gmail, Facebook, etc.