¿El fin de las contraseñas?

André Goujon

Especialista de Awareness & Research

25/03/2013 – version 1.1

Índice

Introducción

Para evitar que otros puedan acceder a recursos privados, la protección de los mismos se convirtió en una conducta esencial de las personas y la sociedad.. En este sentido, resulta interesante destacar que hace aproximadamente 4.000 años se inventó el primer sistema de cerradura construido a partir de madera y, en la actualidad, es impensado que un automóvil, casa, tienda, oficina, etc. no posean algún sistema de protección que evite que un tercero no autorizado pueda acceder a ellos.

Con los sistemas informáticos sucede algo similar. Tanto las personas como las empresas almacenan información importante y confidencial que de caer en las manos equivocadas, podría resultar problemático. Por ello, el uso de credenciales de acceso, como nombre de usuario y contraseña, son una parte fundamental de servicios como el correo electrónico, las redes sociales, y los recursos compartidos de red, entre otros.

Por otro lado, y considerando que las credenciales de acceso protegen datos relevantes, existen personas interesadas en vulnerar los sistemas para acceder a los recursos. Aunque el uso de un nombre de usuario y contraseña por sí solo (sistema conocido como autenticación simple) otorga una capa de protección considerable, es sabido que los ciberdelincuentes cuentan con una amplia gama de herramientas capaces de vulnerar claves. Es por ello que cada vez resulta más imprescindible la implementación de un sistema de doble autenticación.

La doble autenticación se trata de un sistema que además de requerir una autenticación simple, como por ejemplo, nombre de usuario y contraseña; solicita el ingreso de un segundo mecanismo, como un código de identificación. Generalmente, este código se envía a un dispositivo del usuario, como un teléfono celular, para que luego, pueda ingresarlo para poder validarse en el equipo. En este sentido, y considerando que la doble autenticación es significativamente más segura que la simple, ¿se tratará del fin de las contraseñas tal y como se conocen en la actualidad?

Robo de claves y malos hábitos

Como se mencionó en la introducción, el uso de la autenticación simple otorga un cierto nivel de protección, sin embargo, a raíz del avance tecnológico y el aumento en el interés de los atacantes por obtener información confidencial, las credenciales de acceso simples son cada vez menos efectivas para brindar un nivel de seguridad adecuado.

En primer lugar, y junto con el avance tecnológico de las CPU y GPU (Unidad de Procesamiento de Gráficos), vulnerar una contraseña a través de ataques de fuerza bruta, es decir, aquellos que buscan inferir la contraseña a través de diccionarios de datos, resulta considerablemente más rápido y sencillo que hace algunos años. En este sentido, un clúster de 25 GPU es capaz de descifrar contraseñas de ocho caracteres en cinco horas y media. Asimismo, si se aumenta el número de GPU, el tiempo necesario para descifrar una clave será incluso menor. Aunque implementar contraseñas de diez o más caracteres dificulta que un atacante pueda obtener acceso, esto no siempre soluciona el problema de forma satisfactoria.

Este inconveniente se agrava aún más si se considera que existen otros ataques informáticos capaces de vulnerar contraseñas. Casos de phishing, una amplia gama de códigos maliciosos, y otros ataques dirigidos específicamente en contra de empresas puntuales han demostrado empíricamente que la autenticación simple es cada vez más vulnerable.

Robo de contraseñas mediante ataques específicos: casos como Yahoo!, Twitter y LinkedIn

Uno de los primeros ataques que involucró el robo masivo de contraseñas fue el ocurrido con la famosa red laboral LinkedIn. El incidente tuvo como consecuencia el robo de 6.5 millones de claves de usuarios de esta red social y la publicación de dicha información en un foro ruso. Por su parte, los responsables de LinkedIn decidieron implementar una segunda capa de seguridad al momento de almacenar las contraseñas en los servidores, conocida como granos de sal, una técnica que permite agregar información aleatoria a las claves. Esta medida busca reforzar el algoritmo criptográfico SHA implementado por esta red social.

Otro ataque similar fue el ocurrido en contra de Yahoo!; en este caso, un grupo de atacantes denominados D33Ds Company lograron vulnerar algunos sistemas de la empresa mediante una inyección SQL, con lo que consiguieron robar 450.000 credenciales. Ese mismo 12 de julio de 2012, se daba a conocer otro caso parecido en contra de Formspring, red social de preguntas y respuestas. En esa ocasión, los atacantes robaron 420.000 credenciales de acceso. Como medida cautelar, la empresa afectada decidió restablecer las contraseñas de todos sus usuarios (28 millones en aquel momento) y afirmó haber resuelto la vulnerabilidad que habría permitido el ingreso de los atacantes.

Un ataque más reciente es el que sufrió Twitter, donde se vulneraron las cuentas de 250,000 usuarios. Aunque la empresa afectada no concedió más detalles sobre el incidente, les recomendó a los usuarios desactivar el plugin de Java como medida de precaución. Este incidente se suma a otro en donde la misma red social, tuvo que realizar un restablecimiento masivo de cuentas debido a una posible brecha de seguridad.

A pesar de que adoptar las medidas necesarias para almacenar contraseñas de forma segura, como el cifrado mediante bcrypt o SHA y granos de sal, son esenciales para prevenir estos ataques, la implementación de un sistema de doble autenticación permite mitigarlos considerablemente.

Por ejemplo, impediría que los atacantes puedan acceder a las cuentas debido a que desconocerían el segundo factor (por ej. PIN) para poder identificarse en el sistema.

Robo de contraseñas corporativas mediante códigos maliciosos

Actualmente, casi la totalidad de los códigos maliciosos están diseñados para robar algún tipo información, por lo tanto, prácticamente cualquier servicio o recurso protegido por credenciales de acceso, podría ser vulnerado si el usuario inicia sesión en un sistema infectado. En estos casos es importante destacar que el robo de la contraseña ocurre en la computadora de la persona y no en el entorno informático de la empresa proveedora del servicio.

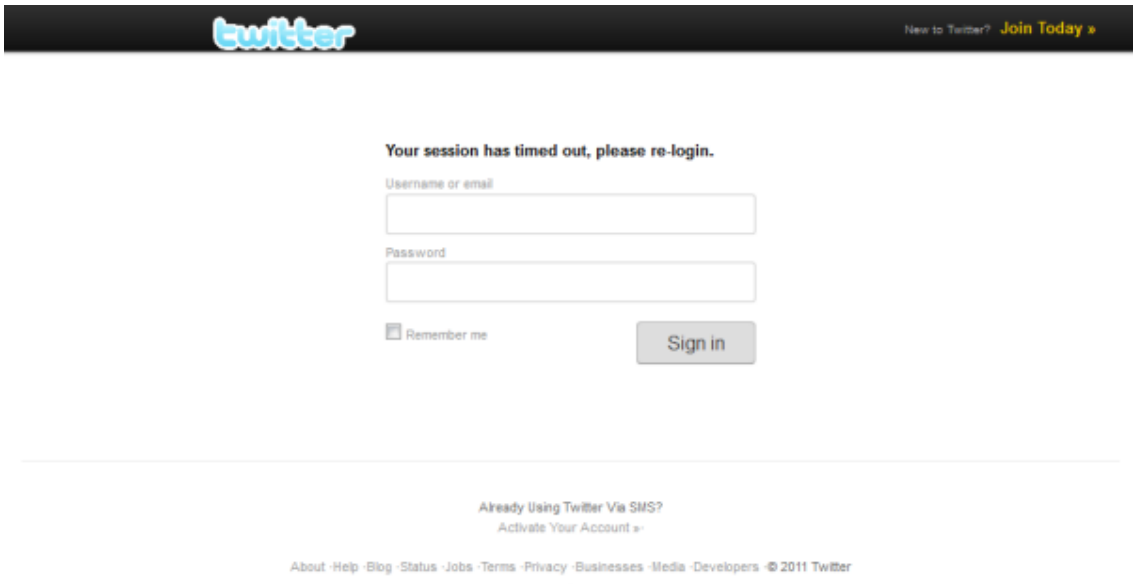
Podemos tomar como ejemplo el caso de Dorkbot, un gusano que se propagó intensamente en América Latina, que reclutó al menos 80.000 computadoras zombis en la región y logró robar más de 1.500 cuentas corporativas de correo electrónico. En otras palabras, los cibercriminales responsables de este ataque tuvieron acceso total a la información almacenada en mensajes y archivos adjuntos. Esto representa un serio problema para el funcionamiento de la red corporativa, el consiguiente deterioro de la imagen del negocio y el robo de datos confidenciales.

Dorkbot es una amenaza que posee un campo amplio de acción, es decir, casi cualquier usuario que se infecte es de utilidad para el cibercriminal. Asimismo, mientras más personas resulten afectadas por este malware, mejor será para el atacante. Por otro lado, existen algunos códigos maliciosos dirigidos y específicos. Se trata de amenazas desarrolladas para atacar a un blanco mucho más reducido como una empresa en particular o incluso un país determinado. Los atacantes buscan afectar solo al grupo objetivo y cualquier víctima adicional podría contribuir a que la amenaza sea descubierta con mayor celeridad, por lo tanto, tienden a evitar tal situación. El peligro de estos ataques radica en la dificultad para detectarlos y en la cantidad de información que pueden llegar a robar. Como se puede apreciar, los ciberdelincuentes harán todo lo posible para robar información, ya sea a través de códigos maliciosos destinados a múltiples objetivos, o mediante *malware* diseñado para atacar a blancos más específicos. En esta línea, un sistema de doble autenticación permitiría otorgar una capa de protección adicional al evitar que los ciberdelincuentes puedan acceder directamente al correo electrónico y otros servicios protegidos por usuario y contraseña.

Robo de contraseñas mediante phishing

El phishing es otro ataque informático que utilizan los cibercriminales para obtener credenciales de acceso de servicios bancarios, redes sociales, correo electrónico, entre otros. Se trata de una modalidad de fraude electrónico en la que el ciberdelincuente suplanta a una entidad para solicitarle a la víctima datos sensibles como nombres de usuarios, contraseñas, tarjetas de crédito, de coordenadas, etc. De acuerdo a una encuesta realizada por ESET Latinoamérica, los servicios más suplantados por los cibercriminales a través del phishing son el webmail (correo electrónico en línea) con 46%, redes sociales con 45%, y bancos 44%.

A continuación se muestra la captura de un ataque de phishing que logró robar 31.000 cuentas de Twitter:



Tal como se puede apreciar, el sitio fraudulento luce idéntico al genuino de Twitter. Además, se le informa falsamente a la potencial víctima que ingrese sus credenciales de acceso debido a que la sesión habría expirado. A diferencia de los códigos maliciosos, en el phishing es el propio usuario quien, una vez que ha sido engañado, facilita la información a los atacantes. En este caso un sistema de doble autenticación impediría que los cibercriminales accedan a la cuenta debido a que no conocerían el código numérico necesario para ingresar. De acuerdo a la misma encuesta llevada a cabo por ESET Latinoamérica, los datos más solicitados por los cibercriminales son los nombres de usuario y contraseñas con el 81% de las preferencias. Considerablemente más atrás quedan los *token* (dispositivos físicos que generan números de acuerdo a un patrón) con un 9%. Este porcentaje demuestra que los ciberdelincuentes no están interesados en obtener este tipo de información debido a que el código generado por un sistema de doble autenticación tiene una validez limitada y cambia constantemente. Este aspecto resulta fundamental para dificultar que un tercero pueda acceder a un servicio protegido por un sistema de estas características.

Las conductas inseguras del usuario

En las secciones anteriores se mencionaron ataques capaces de vulnerar sistemas de autenticación simple, sin embargo, existen otros aspectos más allá de las amenazas informáticas que pueden facilitar el acceso de un tercero a información confidencial. Frente a determinados ataques, una contraseña de una longitud de diez o más caracteres puede proporcionar un nivel de seguridad extra, no obstante, esta situación también provoca comportamientos inadecuados por parte de los usuarios. Muchas personas suelen utilizar una contraseña única para todos los servicios, lo que facilita considerablemente que un atacante pueda acceder a todos los recursos protegidos con esa clave. A continuación, se expone una tabla con los cinco problemas más recurrentes con respecto a las contraseñas y los usuarios:

Problema	Impacto
Uso de una contraseña única para varios servicios:	Facilita el acceso de un atacante a varios servicios y recursos con tan solo robar una única clave.
Contraseñas idénticas para uso personal y laboral:	Facilita el acceso de un atacante tanto a las cuentas personales de la víctima como a los recursos corporativos.
Uso de contraseñas cortas:	Cualquier contraseña que posea menos de diez caracteres posibilita que un tercero pueda vulnerarla a través de ataques de fuerza bruta.
Utilización de contraseñas fáciles de adivinar:	Para evitar el olvido de las claves, algunos usuarios implementan contraseñas fáciles de adivinar como palabras típicas, secuencias numéricas (12345, 54321, 0000, etc.), fechas, etc. Tal situación aumenta considerablemente la posibilidad que un tercero pueda descifrar la clave.
Contraseñas anotadas en papeles o documentos:	Para evitar el olvido de las claves, algunos usuarios escriben las credenciales de acceso en el teléfono, en un documento, en hojas, etc. Cualquier persona que tenga acceso al lugar en donde se encuentre escrita la contraseña podrá acceder a los recursos protegidos.

Tabla 1 Comportamientos inseguros de los usuarios con las contraseñas.

Si bien al evitar estas situaciones se puede lograr un nivel de seguridad superior, un sistema de doble autenticación permitiría aumentar incluso más el grado de protección disponible.

Sistemas de autenticación

Los sistemas de autentificación son todos aquellos métodos diseñados para verificar la identidad de un usuario con el objetivo de otorgarle acceso a un recurso protegido según corresponda. Siempre requieren del uso de al menos un factor de autenticación para poder reconocer a la persona.

En este sentido, la autenticación simple a través de nombre de usuario y contraseña es uno de los métodos de protección más utilizados en la actualidad, sin embargo, al requerir un solo factor de autenticación, se convierte en un procedimiento significativamente más vulnerable. A continuación, se explica en qué consiste cada factor:

Factor de conocimiento (algo que sé)

Se trata de algo que el usuario sabe y conoce. Por ejemplo: contraseñas, números PIN, patrones, secuencia, etc.

Factor de posesión (algo que tengo)

Es algo que el usuario posee como un teléfono inteligente, un *token*, tarjeta ATM, etc. Estos dispositivos suelen utilizarse para el envío de códigos que sirven para identificar al usuario en un sistema.

Factor de inherencia (algo que soy)

Se trata de rasgos conductuales y físicos intrínsecos al ser humano y que permiten identificarlo unívocamente a través de la biometría. Las huellas dactilares, el iris, el rostro y la retina son algunos ejemplos.

Sistema de doble autenticación

Los sistemas de doble autenticación, son aquellos que requiere del ingreso de dos de los tres factores de autenticación para poder identificar y permitir el acceso de un usuario a un recurso o servicio. A diferencia de la autenticación simple busca evitar que un atacante pueda adulterar y suplantar su identidad ingresando credenciales robadas.

En los siguientes esquemas se puede apreciar la diferencia con mayor nitidez:

Ilustración 1 Sistema de autenticación simple

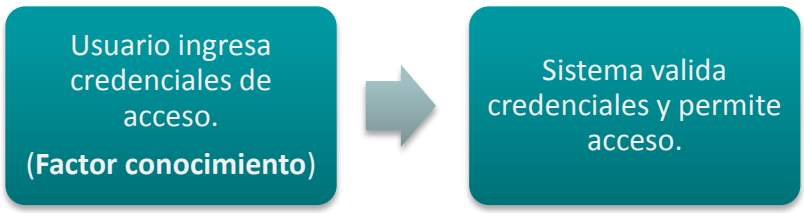
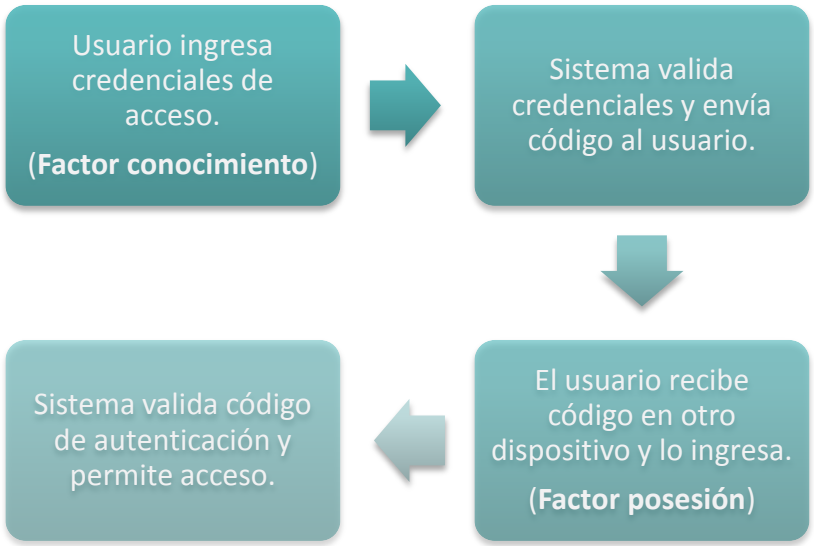


Ilustración 2 Sistema de doble autenticación



En la mayoría de los casos, los sistemas de doble autenticación utilizan códigos numéricos como segundo factor de comprobación. El objetivo es que el usuario reciba dichos dígitos en algún dispositivo que tenga en su poder como un teléfono inteligente o un *token*. Posteriormente, deberá ingresar ese número para poder iniciar la sesión. A continuación, se detallan las características más relevantes de estos códigos:

- El código que recibe el usuario en su dispositivo podrá ser utilizado solo una vez (*OTP – One-time password*). Esto garantiza un mayor nivel de seguridad al evitar que dicho número pueda reutilizarse por parte de terceros.
- El código expira transcurrido un tiempo determinado.
- El código cambia aleatoriamente cada vez que el usuario necesita ingresar al servicio o recurso.

Aunque existen algunos códigos maliciosos para teléfonos inteligentes que son capaces de robar el segundo factor de autenticación, las características expuestas anteriormente permiten mitigar el riesgo de que un cibercriminal emplee *malware* para vulnerar un sistema de este tipo.

Activar doble autenticación en servicios

Ciertos servicios de correo electrónico, redes sociales y otros, implementan sistemas de doble autenticación para resguardar la seguridad de los usuarios, sin embargo, dicha opción por lo general, se encuentra desactivada de forma predeterminada. En la siguiente tabla, se exponen los servicios que implementan doble autenticación y se detallan las instrucciones para poder activar esta característica:

Servicio	Instrucciones
Google	Para activar la doble autenticación en una cuenta de Google es necesario seguir estos pasos: Iniciar sesión y acceder al siguiente enlace: Verificación en dos pasos. Allí se debe presionar el botón "Iniciar configuración". Se deberán seguir las instrucciones que aparecerán en pantalla. Más información.
Gmail	Iniciar sesión en la cuenta de Gmail de modo normal. Ir al botón en forma de rueda dentada y presionar sobre "Configuración". Se debe hacer clic en la pestaña "Cuentas e importación" y luego sobre el enlace "Otra configuración de la cuenta de Google". Allí presionar sobre "Seguridad" y luego hacer clic en el botón "Configuración" que aparece en la sección Verificación en dos pasos. Más información.
Facebook	Iniciar sesión en Facebook y presionar sobre el botón en forma de rueda dentada. Allí hacer clic en "Configuración de la cuenta". Posteriormente presionar sobre "Seguridad" e ir a la sección "Aprobaciones de inicio de sesión" y hacer clic en editar. Se deberá seguir las instrucciones que aparecen en pantalla. Más información.
Dropbox	Iniciar sesión en la cuenta de Dropbox. Hacer clic en el nombre del usuario en la parte superior derecha de la página y presionar sobre "Configuración". Allí presionar sobre el botón" Seguridad" También se puede hacer clic sobre este enlace. En la parte que dice "Inicio de sesión de cuenta" hacer clic en el enlace "Cambiar" que aparece al lado derecho de "Verificación en dos pasos". Más información.
Bancos	Activar la doble autenticación en este tipo de cuentas es una medida recomendada para mejorar la seguridad de las transacciones bancarias. Dependiendo de la entidad las instrucciones podrían variar. Recomendamos consultar con su banco sobre la disponibilidad de este servicio.

Tabla 2 Instrucciones para activar doble autenticación en servicios.

Conclusión: ¿El fin de las contraseñas?

A lo largo de este artículo se han expuesto y explicado las diversas razones que demuestran que la autenticación simple no es un método lo suficientemente robusto para proteger adecuadamente un recurso o servicio. Entre los casos más relevantes que tienden a vulnerarlo rápidamente se pueden encontrar: códigos maliciosos que roban credenciales de acceso, ataques específicos en contra de empresas, casos de phishing y las conductas inseguras que algunos usuarios adoptan con respecto al manejo de claves.

En vista de todos los aspectos mencionados anteriormente, resulta imperioso implementar un sistema de doble autenticación, sin embargo, esto no implica que las credenciales de acceso como nombre de usuario y contraseña dejen de utilizarse. Por el contrario, formarán parte integral de un sistema de doble autenticación. Cabe destacar que, algunos sitios como Facebook, Google, Gmail, Dropbox, entre otros, ya cuentan con estos mecanismos.

Por otro lado, algunas entidades bancarias también han implementado este tipo de sistemas en reemplazo de la tarjeta de coordenadas, ya que si bien otorga mayor seguridad, posee una cantidad limitada de combinaciones. En este sentido, en el Laboratorio de Investigación de ESET Latinoamérica se han observado ataques de phishing en donde los atacantes les solicitaron a las víctimas todos los números de las tarjetas de coordenadas como parte del fraude. Si la persona envía dicha información, la seguridad adicional que otorga este sistema se ve completamente comprometida. Casos como el phishing que afecto a un importante banco de Panamá y otro dirigido a usuarios brasileños demuestran fehacientemente que los cibercriminales solicitan estos datos para obtener rédito económico. Un sistema de doble autenticación es considerablemente más difícil de vulnerar debido, entre otros motivos, a que la cantidad de combinaciones numéricas es ampliamente mayor y no pueden visualizarse de una sola vez.

Independientemente de la implementación de estos mecanismos y otras formas de protección, el factor educativo resulta fundamental para poder prevenir ataques. Un entorno informático protegido adecuadamente no es solo aquel que implementa la mejor tecnología disponible en el mercado, sino el que también considera la educación de los usuarios como parte fundamental en el proceso de protección.