TECNOTREND

AUTENTIFICACIÓN MULTI-FACTOR PARA REDUCIR LOS RIESGOS DE SEGURIDAD

Mtro. Rosendo Ayala Vaca

Maestro en Redes y Seguridad de la Información, Ingeniero en Telemática. Administrador de Infraestructura de TICs, en Universidad Quetzalcóatl en Irapuato (México), donde trabaja con temas como la administración de sistemas y servidores en Windows, Linux Centos y Ubuntu, FreeBSD; administración de redes de datos y telefonía; administración de enlaces dedicados de internet; administrador de servicios WEB, SFTP, DNS, DHCP; administrador de Help Desk. Diseñador de OLA's y SLA's del departamento; administrador de software Contpaq del área administrativa y laboratorios; soporte Técnico nivel 2 y asesorías a usuarios administrativos, profesores y alumnos.

Resumen

Los passwords y otros medios de autenticación basados en *"Something you know"* son débiles por falta de cultura en seguridad de la información. Por lo que es recomendable utilizar un factor de autenticación adicional para robustecer la seguridad de los sistemas. La autenticación multi-factor puede ser implementada a nivel de red o a nivel de aplicación/sistema.

Summary

Passwords and other means of authentication based on "Something you know" are vulnerable due to lack of information. It is prudent to use additional authentication to strengthen the security of the systems. Multi-factor authentication can be implemented at the network level or the application/system level.

Palabras clave

Autenticación Multi-Factor, aplicaciones móviles, criptografía, passwords, something you know, Seguridad de la Información.

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Keywords

Multi-factor authentication, mobile applications, cryptography, passwords, something you know, Information Security.

Introducción

Cuando se ingresa en un servicio con un usuario y contraseña, se están utilizando dos datos: el primero es un identificador público y el segundo es una clave privada desconocida por los demás. Las preguntas a hacerse son ¿qué tan segura es esa clave privada?, ¿qué pasa si alguien más adivina o consigue la contraseña por algún medio?, ¿se puede proteger la integridad y confidencialidad aun cuando se dejó de ser la única persona con conocimiento de la clave de acceso?

El uso de passwords no es nada nuevo. Ha existido por siglos desde antes de que llegara la era digital. El ejército romano ya utilizaba contraseñas para distinguir a los aliados de los enemigos. Sin embargo, con la velocidad a la que crece la tecnología, la velocidad de procesamiento de los nuevos equipos y la cantidad de información que se almacena en medios digitales, el uso de contraseñas ya no es suficiente para proteger la información y su privacidad, como revelaron investigaciones recientes elaboradas por CSIDentity y WeLiveSecurity.

Por ese motivo es necesario dar un salto y autenticar la identidad por más de un mecanismo de seguridad, por el bien de la información. Con la autenticación MFA (*Multi-Factor Authentication*, Autenticacion Multi-Factor) se pude hacer uso de una computadora portátil, tablet, teléfono móvil o cualquier otro dispositivo móvil compatible (BYOD, *Bring your own device*) para agregar un punto adicional a la seguridad

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Metodología

Para poder controlar el acceso a una aplicación informática es necesario probar la identidad de quien esté utilizando el dispositivo o sistema. Los principales mecanismos de seguridad para identificar a un usuario están basados en:

- SYK (*something you know,* algo que el usuario conoce): Por ejemplo, los passwords, PIN's, respuestas a preguntas, frases secretas de seguridad, patrones de desbloqueo y desbloqueo basado en imágenes.

- SYH (*something you have,* algo que el usuario tiene): Un dispositivo token, una smart card, una tarjeta de proximidad, un teléfono móvil, una llave USB, un certificado digital, por mencionar algunos.

- SYA (*something you are,* algo que el usuario es): Las características biométricas del individuo que lo hacen único; las principales y más utilizadas son las huellas dactilares, el iris, el rostro, el timbre de voz y la firma.

El mecanismo más utilizado en la era informática ha sido SYK (algo que el usuario conoce) mediante el uso de passwords, desde que en 1960 Fernando Corbato introdujo la idea para poder utilizar un mainframe común que tenían que compartir los investigadores del MIT (*Massachusetts Institute Technology*), permitiendo con el uso de una cuenta de usuario y password el acceso exclusivo de cada usuario a sus propios archivos.

El problema más grave que tiene este mecanismo de seguridad es que algo que el usuario sabe es también algo que puede olvidar por lo que se requiere un método de recuperación (la respuesta secreta se ha utilizado por décadas), dando

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

otro punto vulnerable a un ataque. Otro punto débil es que SYK es algo que nadie más debe conocer, adivinar o extraer.

En el año 2004, Bill Gates predijo la muerte del password como método de autenticación por no cumplir con el desafío de mantener la información segura. Esta predicción se debió a los malos hábitos ya entonces conocidos en el uso de passwords por parte de los usuarios en donde generan contraseñas sencillas y de longitud mínima para no olvidarlas, las anotan en un post-it y este lo pegan en el escritorio, las anotan en una hoja de papel o la guardan un archivo del mismo equipo, sin seguridad. Si se suma a esto que el 61 % de los internautas usan el mismo password en múltiples sitios a los que están registrados (Yahoo, Hotmail, Gmail, Facebook, twitter, Instagram, entre otros) y un 44 % tarda más de un año en cambiar de password se puede ver el porqué es el mecanismo más vulnerable y ampliamente atacado por troyanos, keyloggers, ataques de fuerza bruta, ataques de diccionario, Phishing, Pharming u otros métodos de ingeniería social.

Al realizar una comparativa entre los estudios sobre los hábitos en passwords por CSID (2012) y Guccione (2017), se revela que las conductas de los usuarios de un servicio no han cambiado significativamente en los últimos años al preferir el uso de contraseñas cortas, simples y nemónicas. Pastorino (2017), expone que en las diferencias del año 2016 en comparación con el 2017 los usuarios intentaron hacer un esfuerzo mínimo por cambiar su contraseña utilizando los mismos passwords predecibles de antes, con algunos pequeños cambios para cumplir con las auditorias básicas de seguridad actuales (el uso de mayúsculas, minúsculas, números) y así el sistema acepte como válidos los passwords. Por ejemplo, cambiando la contraseña “password” por “Password1234” o “qwerty” por “Qwerty01!”.

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

Tabla 1

Los 25 passwords más utilizados en el año 2016.

RANK	PASSWORD
1	123456
2	123456789
3	Qwerty
4	12345678
5	111111
6	1234567890
7	1234567
8	Password
9	123123
10	987654321
11	Qwertyuiop
12	Mynoob
13	123321
14	666666

Fuente:
https://keepersecurity.com/blog/2017/01/13/most-common-passwords-of-2016-research-study/

Por el otro lado, los sistemas y servidores deben hacer uso de protocolos criptográficos y hashes seguros para proteger los passwords y evitar otros tipos de ataques conocidos como el de tabla rainbown que permite comparar hashes de contraseñas.

La PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago, *Payment Card Industry - Data Security Standard*) en su norma 3.2 recomienda el uso de por lo menos dos factores para asegurar que no hay personas curiosas o malintencionadas accediendo a información privada, pero esta norma no se limita a las transacciones del sector bancario, las fintech y el comercio electrónico ya que los datos confidenciales y la privacidad no son exclusivos de los rubros financieros. Para Bissada & Olmsted (2018), la autenticación multi-factor ha conseguido reducir los riesgos de seguridad en el

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

uso de servicios cotidianos como la computación, los dispositivos móviles y los sistemas de acceso, al igual que se encuentra presente en nuevas áreas como la telemedicina, el gobierno electrónico y, en un futuro cercano, en el voto móvil.

Resultados

En la actualidad, para conseguir una autenticación realmente segura es necesario agregar al factor de SYK, por lo menos otro de los mecanismos de seguridad (SYH "something you have" o SYA "something you are"). Aun cuando el usuario puede también perder el objeto o cualidad que lo hace único para autenticarse ante un sistema y tendría que realizar un proceso alterno y probablemente complejo para identificarse y cambiar sus credenciales de acceso, estos otros mecanismos son menos vulnerables a ataques externos. La persona que obtuviera el objeto de autenticación (segundo factor) o lograra sustraer o coincidir en un rasgo (tercer factor) no podría acceder sin conocer el primer factor. La autenticación MFA es indispensable para reforzar la seguridad en cualquier sistema que requiera una autenticación segura y de paso lograr el concepto de no repudio en el que el usuario no puede negar que fue él quien se identificó dos o más veces en el sistema.

Conclusiones

Ya no es posible basar la seguridad de la información confidencial en un solo mecanismo de autenticación y menos en el de SYK por la debilidad de los passwords.

Es importante aclarar que MFA reemplaza el término 2FA (Autenticación en 2 factores) y no limita al permitir 2 o más factores.

El objetivo fundamental de la MFA es robustecer la seguridad de una aplicación o dispositivo al crear una defensa por capas y hacer que sea más difícil para una

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203

persona no autorizada acceder a un objetivo. Si uno de los factores se ve comprometido o se rompe, independientemente de cuál hubiere sido, la persona no autorizada todavía tiene al menos otra barrera más que saltar antes de entrar al sistema.

El uso de una MFA es muy diverso, se puede aplicar en la banca electrónica, el ecommerce, o en proyectos nuevos como el e-voting y las fintech.

Referencias:

Bissada, A., & Olmsted, A. (2018). Mobile multi-factor authentication. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (págs. 210-211). Cambridge, UK: IEEE.

CSID. (2012). Consumer Survey: Password Habits. A study of password habits among American consumers. Obtenido de https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

Guccione, D. (13 de Enero de 2017). What the Most Common Passwords of 2016 List Reveals [Research Study]. Recuperado el 25 de 04 de 2018, de What the Most Common Passwords of 2016 List Reveals [Research Study]

Pastorino, C. (24 de 05 de 2017). Estadísticas y reglas para predecir contraseñas: ¿es obsoleta la fuerza bruta? Obtenido de We Live Security: https://www.welivesecurity.com/la- es/2017/05/24/obsoleta-fuerza-bruta-predecir-contrasenas/

Año 2018 ISSN 2448-8496 Universidad De La Salle Bajío A.C.
Reserva de Derechos al Uso Exclusivo No. 04 – 2016 – 113013104700 – 203