https://repository.uaeh.edu.mx/revistas/index.php/xikua/issue/archive

XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan

Publicación semestral, Vol. 11, No. 22 (2023) 39-43

ISSN: 2007-4948

Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación

Security in Authentication Systems: Vulnerability Analysis and Mitigation Strategies

Isai V. Marmolejo-Corona [a], *Fernando A. Bautista-Aguilar* [b], *Yahir F. Santiago-González* [c], *Gerardo A. Serrano-Manzano* [d]

Abstract:

The article discusses online authentication systems, specifically single-factor authentication (SFA) and two-factor authentication (2FA). Vulnerabilities of these systems, such as phishing attacks and message interception, are discussed and strategies to mitigate these risks, such as the implementation of strong passwords, user training, multifactor authentication, biometric authentication and regular updates, are proposed. The importance of collaboration between service providers and users to ensure online security is stressed. Several reliable sources are cited to support the information presented. Overall, the paper provides a detailed and comprehensive overview of online authentication systems and how they can be improved to enhance online security.

Keywords:

Authentication, computer security, systems, users, data protection

Resumen:

El artículo analiza los sistemas de autenticación en línea, en concreto la autenticación de factor único (SFA) y la autenticación de dos factores (2FA). Se discuten las vulnerabilidades de estos sistemas, como los ataques de phishing y la interceptación de mensajes, y se proponen estrategias para mitigar estos riesgos, como la implantación de contraseñas seguras, la formación de los usuarios, la autenticación multifactor, la autenticación biométrica y las actualizaciones periódicas. Se subraya la importancia de la colaboración entre proveedores de servicios y usuarios para garantizar la seguridad en línea. Se citan varias fuentes fiables para respaldar la información presentada. En general, el ensayo ofrece una visión detallada y completa de los sistemas de autenticación en línea y de cómo pueden mejorarse para aumentar la seguridad en línea.

Palabras Clave:

Autenticación, seguridad informática, sistemas, usuarios, protección de datos

Introducción

Con la creciente importancia de la seguridad en línea, la autenticación se ha convertido en una herramienta clave para proteger los sistemas informáticos y la información que contienen. La autenticación es un proceso mediante el cual se verifica la identidad de un usuario que intenta acceder a un sistema o información específicos. Los

[a] Isai V. Marmolejo-Corona, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-1299-5052, Email: ma367093@uaeh.edu.mx

[b] Fernando A. Bautista-Aguilar, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-9158-2004, Email: ba466658@uaeh.edu.mx

[c] Yahir F. Santiago-González, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-4797-6134, Email: sa464030@uaeh.edu.mx

[d] Gerardo A. Serrano-Manzano Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0001-7261-7243, Email: se465780@uaeh.edu.mx

Fecha de recepción: 24/03/2023, Fecha de aceptación: 10/05/2023, Fecha de publicación: 05/07/2023

DOI: https://doi.org/10.29057/xikua.v11i22.10802

sistemas de autenticación se utilizan habitualmente para proteger información sensible e impedir el acceso no autorizado a sistemas y redes.

Entre los sistemas de autenticación más comunes se encuentran la autenticación de factor único (SFA) y la autenticación de dos factores (2FA). SFA es un sistema que utiliza una única forma de autenticación, normalmente una contraseña, para verificar la identidad de un usuario. Por otro lado, 2FA es un sistema que utiliza dos formas de autenticación, como una contraseña y un código enviado a un dispositivo móvil, para verificar la identidad de un usuario.

Aunque estos sistemas son útiles para garantizar la seguridad en línea, presentan ciertas vulnerabilidades que pueden ser explotadas por atacantes malintencionados. En este ensayo se analizarán estas vulnerabilidades y se propondrán estrategias de mitigación para cada uno de estos sistemas, con el objetivo de mejorar su seguridad y prevenir posibles ataques.

Sistemas de autenticación como proceso para protección de datos

Un sistema de autenticación para ser más concisos se refiere a “un conjunto de procedimientos y protocolos informáticos que se utilizan para verificar la identidad de un usuario y permitirle el acceso a un sistema o servicio”, y bien un proceso necesario para garantizar la seguridad y la privacidad en el mundo digital porque garantiza que solo los usuarios autorizados tengan acceso a información o recursos protegidos. Hay varias formas de clasificar los sistemas de autenticación, pero una común es si se basan en lo que el usuario sabe. [3]

Si hablamos de los antecedentes de estos sistemas estaríamos hablando de la época de la antigua Roma en la que se solían utilizar sellos para dar validez a la autenticidad de los documentos. A lo largo del tiempo este tipo de sistemas se han adaptado a nuevas necesidades de la sociedad moderna, algo que ha impulsado este cambio es la revolución digital por la necesidad de proteger la integridad de la información que se encuentra dentro de una red. De los primeros sistemas de este tipo y de los más conocidos hasta la actualidad es el *Single-Factor Authentication (*SFA), consiste en un usuario y una contraseña estas forman parte del proceso del sistema en el que tenemos tres objetos o sujetos interactúan la cuenta, la llave y el usuario explicado en diagrama 1, sin embargo este sistema fue y es vulnerado fácilmente poniendo en riesgo la información de los usuarios de lo cual nace en *Two-Factor Authentication*(2FA) y la autenticación biométrica, cuyas tecnologías ahora se basan ahora en proporcionar diferentes formas para acceder a una cuenta ahora incluyendo como parte del proceso un nuevo objeto “teléfono móvil”, este objeto actúa como una segunda llave en la que es generada un *token* “código o una serie de caracteres que se genera de manera aleatoria”[1] y de la misma forma en la que ingresamos una contraseña el *token* se ingresa y se válida para darte autorización al servicio diagrama 2. Por otro lado, el uso de datos biométricos utiliza características físicas y únicas del usuario tal como las huellas dactilares o reconocimiento facial aunado a esto se los datos biométricos también son utilizados como un *token* o llave secundaria para acceder a la cuenta. Cabe mencionar que cada método de autenticación tiene sus ventajas y desventajas, y se debe seleccionar el método adecuado según las necesidades de seguridad y la comodidad del usuario. [a]

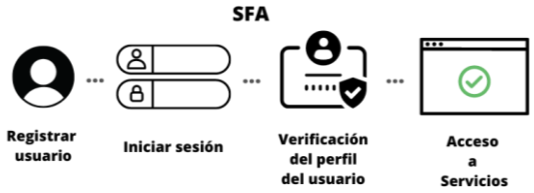

Diagrama 1. *Single-FactorAuthentication* (SFA). [b]

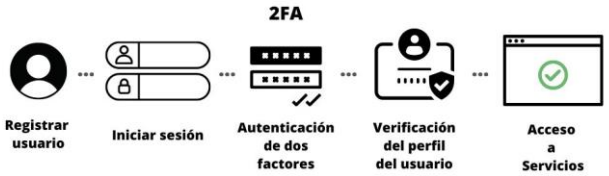

Diagrama 2. *Two-Factor Authentication* (2FA). [b]

Análisis de vulnerabilidades

La autenticación de factor único (SFA) es el método de autenticación más básico y se basa en la verificación de un único dato, como un nombre de usuario y una contraseña. Aunque es un sistema sencillo y fácil de usar, tiene varias vulnerabilidades que pueden ser explotadas por atacantes malintencionados. Algunas de estas vulnerabilidades son

Contraseñas débiles: Las contraseñas débiles son una de las mayores vulnerabilidades del SFA. Muchos usuarios utilizan contraseñas fáciles de adivinar, como cumpleaños, nombres de familiares o mascotas, lo que las hace vulnerables a ataques de fuerza bruta. Los atacantes pueden utilizar software automatizado para probar miles de posibles combinaciones de contraseñas hasta dar con la correcta, lo que les permite acceder a los sistemas protegidos. [2]

Phishing: Los ataques de phishing son otra vulnerabilidad importante de los SFA. En este tipo de ataque, los atacantes envían correos electrónicos o mensajes de texto falsos para engañar a los usuarios y hacerles revelar sus credenciales de acceso. [5] Estos mensajes pueden parecer legítimos, ya que a menudo se disfrazan de correos electrónicos de empresas o sitios web conocidos, lo que puede engañar a los usuarios desprevenidos para que faciliten información sensible.

Ataques de intermediarios: Los ataques de intermediarios también son una vulnerabilidad común de SFA. En este tipo de ataque, los atacantes interceptan la comunicación entre el usuario y el sistema protegido, lo que les permite obtener acceso no autorizado. Los atacantes pueden utilizar herramientas como redes Wi-Fi públicas inseguras o malware para interceptar la información de inicio de sesión del usuario.

Reutilización de contraseñas: La reutilización de contraseñas es otra vulnerabilidad común del SFA. Muchos usuarios utilizan la misma contraseña para varios servicios y sitios web, lo que significa que, si se compromete una contraseña, se puede acceder a varias cuentas. Esto hace que SFA sea vulnerable a ataques de fuerza bruta y phishing.

Además de los ataques mencionados y por otro lado la Two-Factor Authentication (2FA) también tiene vulnerabilidades relacionadas con la forma en que se implementa. Por ejemplo, si un sitio web utiliza un método de autenticación de dos factores basado en SMS, los atacantes pueden clonar la tarjeta SIM del usuario y redirigir los mensajes de texto a su propio dispositivo. Además, si se utiliza una aplicación de autenticación, el dispositivo del usuario puede verse comprometido por malware o virus, permitiendo a los atacantes acceder a los códigos de seguridad generados por la aplicación. Otro problema relacionado con la 2FA es la falta de compatibilidad con algunos servicios en línea, lo que puede hacer que los usuarios tengan que elegir entre seguridad y comodidad. [5]

Normalmente, una contraseña se combina con un código de seguridad enviado por mensaje de texto o una aplicación de autenticación. Aunque la 2FA es más segura que la SFA, también tiene sus vulnerabilidades. Algunas de estas vulnerabilidades son:

Ataques de ingeniería social: Los ataques de ingeniería social son una de las mayores vulnerabilidades de la 2FA. En este tipo de ataque, los atacantes engañan a los usuarios para que faciliten su información de autenticación, aunque utilicen 2FA.

Interceptación de mensajes: Los mensajes de texto o las aplicaciones de autenticación utilizadas para la segunda etapa de 2FA pueden ser interceptados por atacantes malintencionados. [8] En algunos casos, los atacantes pueden redirigir estos mensajes a sus propios dispositivos y utilizarlos para acceder a las cuentas de los usuarios.
A pesar de estas vulnerabilidades, la 2FA sigue siendo una forma de autenticación más segura que la SFA.

La evolución de los certificados digitales y su impacto en la seguridad en línea

Un certificado digital es un documento electrónico utilizado para verificar la identidad de una persona u organización en Internet. Estos certificados se basan en tecnología criptográfica y se utilizan comúnmente para proteger la privacidad y seguridad de las comunicaciones en línea, como transferencias bancarias y datos personales. Un certificado digital es emitido por una autoridad de certificación responsable de verificar la identidad del registrante del certificado y garantizar la autenticidad de la clave pública asociada con el certificado. [b]

Una vez emitido, un certificado se puede utilizar para cifrar y descifrar datos, firmar documentos digitalmente y verificar la identidad de la persona u organización propietaria del certificado. Los certificados digitales se utilizan ampliamente en transacciones en línea, como compras en línea y banca en línea, así como en comunicaciones gubernamentales y atención médica. Además, son una forma segura de autenticar a los usuarios en sitios web y aplicaciones móviles. [3] Tenga en cuenta que los certificados digitales tienen una fecha de caducidad y deben actualizarse regularmente para que sigan siendo válidos. Además, la seguridad de un certificado digital puede verse comprometida si se compromete la clave privada asociada con el certificado. “También ofrece la posibilidad de firmar un mensaje al colocar una parte de su llave privada (irreconocible claro) en una firma, que actúa como un certificado de autenticidad” [14].

Los certificados digitales tienen un gran impacto en la seguridad en línea porque permiten verificar la identidad de las personas y organizaciones que interactúan en línea y protegen la privacidad y la seguridad de las comunicaciones electrónicas. Algunos de los efectos principales son:

Protección de la privacidad. Los certificados digitales garantizan una transmisión segura de datos y protegen su privacidad en línea. Los datos cifrados con un certificado digital solo pueden ser descifrados por alguien con la clave privada correcta.

Autenticación de identidad. Los certificados digitales proporcionan una forma segura de autenticar las identidades de las personas y entidades que interactúan en Internet. Los sitios web y las aplicaciones móviles que requieren certificados digitales para la autenticación pueden estar seguros de que la persona o entidad que interactúa con ellos es exactamente como dicen que es.

Protección contra el fraude. Los certificados digitales son una herramienta importante para prevenir el fraude en línea porque permiten verificar la autenticidad de los sitios web y las transacciones en línea. Los sitios web falsos se pueden detectar fácilmente si no tienen un certificado digital válido.

Cumplimiento de la ley. Los certificados digitales se utilizan para cumplir con las leyes y regulaciones que requieren autenticación y protegen la privacidad de los datos.
Como resultado, los certificados digitales han tenido un gran impacto en la seguridad en línea al proporcionar una

forma segura de autenticar las identidades de personas y organizaciones en línea, proteger la privacidad y la seguridad de las comunicaciones electrónicas, prevenir el fraude en línea y cumplir con las leyes y regulaciones de privacidad de datos. [d]

Estrategias de mitigación

Para mitigar las vulnerabilidades asociadas con SFA y 2FA, se deben implementar varias estrategias de seguridad. Algunas de estas estrategias son:

Uso de autenticadores de hardware: Los autenticadores de hardware son dispositivos físicos que generan códigos de seguridad para la autenticación. Estos dispositivos son más seguros que los métodos de autenticación basados en SMS o las aplicaciones de autenticación, ya que no pueden ser interceptados por atacantes malintencionados. Además, algunos autenticadores de hardware también pueden incluir funciones como la identificación por huella dactilar y el reconocimiento facial, lo que aumenta aún más la seguridad.

Supervisión continua de la seguridad: Los proveedores de servicios deben supervisar continuamente la seguridad de sus sistemas y redes para detectar y responder a posibles amenazas. Esto incluye la implantación de herramientas de detección de intrusos y la realización periódica de pruebas de penetración para identificar y corregir posibles vulnerabilidades.

Verificación de identidad en varias fases: La verificación de identidad en varias etapas es una estrategia de seguridad que implica la verificación de la identidad del usuario en varias etapas durante el proceso de autenticación. Esto puede incluir la verificación de la dirección IP del usuario, la ubicación geográfica y otros factores que pueden ayudar a confirmar la identidad del usuario.

Aplicación de políticas de acceso seguro: Las políticas de acceso seguro deben implementarse en los sistemas de autenticación para garantizar que sólo los usuarios autorizados tengan acceso a los recursos protegidos. Esto puede incluir la aplicación de políticas de contraseñas seguras, autenticación multifactor y gestión de identidades y accesos.

La autenticación biométrica: es una tecnología cada vez más utilizada en la protección de sistemas y datos sensibles. A diferencia de los sistemas de autenticación basados en contraseñas o códigos de seguridad, que pueden ser vulnerables a ataques de fuerza bruta o phishing, la autenticación biométrica utiliza características físicas únicas difíciles de falsificar, como huellas dactilares, reconocimiento facial, voz o iris, para verificar la identidad de un usuario.Además, los sistemas de autenticación biométrica pueden ser más rápidos y cómodos para los usuarios, ya que no tienen que teclear una contraseña o código de seguridad cada vez que acceden a un sistema o aplicación.

Actualizaciones periódicas: son esenciales para garantizar la seguridad de los sistemas de autenticación. Con frecuencia se descubren nuevas vulnerabilidades y puntos débiles en los sistemas de autenticación existentes, que pueden ser explotados por atacantes malintencionados para comprometer la seguridad del sistema.

Por lo tanto, los proveedores de servicios deben aplicar actualizaciones periódicas para hacer frente a estas vulnerabilidades y debilidades. Esto puede incluir la incorporación de nuevas tecnologías de autenticación, la corrección de errores en el software o la adición de medidas de seguridad adicionales.

Además, las actualizaciones también pueden ser necesarias para cumplir con los requisitos legales o reglamentarios en constante cambio. Por ejemplo, puede haber nuevos requisitos de seguridad que deban incorporarse a los sistemas de autenticación existentes para garantizar el cumplimiento de la normativa.

Es importante destacar que las actualizaciones no sólo deben abordar las vulnerabilidades existentes, sino también anticiparse a posibles amenazas futuras. Por lo tanto, los proveedores de servicios deben estar siempre atentos a las nuevas amenazas y actualizar sus sistemas en consecuencia para garantizar la seguridad a largo plazo de los sistemas de autenticación.

Conclusiones

La autenticación es un componente crítico de la seguridad en línea y es esencial para proteger la información y los sistemas de los usuarios. Aunque la SFA y la 2FA son importantes, hay que reconocer que no son completamente seguras y pueden ser vulnerables a varios tipos de ataques. Para mitigar estos riesgos, es importante aplicar una serie de estrategias de seguridad.

Una de las estrategias clave es la implantación de contraseñas seguras. Las contraseñas deben ser complejas y difíciles de adivinar, lo que significa que deben contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Además, los usuarios deben cambiar sus contraseñas con regularidad para reducir el riesgo de que sus credenciales se vean comprometidas.

La formación de los usuarios también es esencial. Los usuarios deben ser educados sobre los peligros de los ataques de phishing y la importancia de no revelar su información de autenticación a nadie. Además, deben conocer los distintos tipos de vulnerabilidades a las que pueden enfrentarse y cómo protegerse de ellas.

Otra estrategia eficaz es la autenticación multifactor, como la 2FA. Esta medida de seguridad ayuda a aumentar la seguridad y dificulta el acceso no autorizado a sistemas y datos. Además, los proveedores de servicios deben aplicar medidas de seguridad adicionales, como la

supervisión de actividades sospechosas y la limitación del número de intentos de inicio de sesión.

La autenticación biométrica es otra estrategia que está ganando popularidad. Esta tecnología utiliza características físicas únicas, como las huellas dactilares, para verificar la identidad de un usuario. Es difícil de falsificar y se considera más segura que las contraseñas y los códigos de seguridad.

Por último, es esencial mantener actualizados periódicamente los sistemas de autenticación. Los proveedores de servicios deben estar atentos a las nuevas vulnerabilidades y desarrollar parches de seguridad para corregirlas. Los usuarios también deben asegurarse de mantener sus dispositivos y software actualizados para garantizar una seguridad continua.

En conclusión, la seguridad en línea es un esfuerzo conjunto entre proveedores de servicios y usuarios. La implantación de contraseñas seguras, la formación de los usuarios, la autenticación multifactor, la autenticación biométrica y las actualizaciones periódicas son estrategias eficaces para hacer frente a las vulnerabilidades de autenticación y garantizar la seguridad de los sistemas y la información.

Referencias

[1] BBVA. Te ayudamos a descubrir qué es un 'token' y para qué sirve [Internet]. BBVA; 2023 Feb 10 [citado 2023 Feb 17]. Disponible en: https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/

[2] IBM. Conceptos de seguridad: Identificación y autenticación [Internet]. IBM; s.f. [citado 2023 Feb 17]. Disponible en: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm

[3] Nidecki TA. Authentication and Access Control in Web Applications [Internet]. Toptal; s.f. [citado 2023 Feb 17]. Disponible en: https://www.toptal.com/security/authentication-and-access-control-in-web-applications

[4] Podgorny A. Authentication, Authorization, and Accounting (AAA) in Computer Networks [Internet]. Cisco; s.f. [citado 2023 Feb 17]. Disponible en: https://www.cisco.com/c/en/us/support/docs/security/authentication-authorization-accounting-aaa/13851-10.html

[5] Patil S. Secure User Authentication in Web Applications [Internet]. Imperva; s.f. [citado 2023 Feb 17]. Disponible en: https://www.imperva.com/learn/application-security/user-authentication/

[6] Parecki A. OAuth 2.0 [Internet]. OAuth; s.f. [citado 2023 Feb 17]. Disponible en: https://oauth.net/2/

[7] OASIS. SAML: Security Assertion Markup Language [Internet]. OASIS; s.f. [citado 2023 Feb 17]. Disponible en: https://www.oasis-open.org/standards#samlv2.0

[8] The Password Hashing Competition. Password Hashing Competition [Internet]. The Password Hashing Competition; s.f. [citado 2023 Feb 17]. Disponible en: https://password-hashing.net/

[9] National Cyber Security Centre (NCSC). Multi-Factor Authentication (MFA) [Internet]. NCSC; s.f. [citado 2023 Feb 17]. Disponible en: https://www.ncsc.gov.uk/collection/multi-factor-authentication

[10] Kukic A. Authentication and Authorization with JWT [Internet]. Auth0; s.f. [citado 2023 Feb 17]. Disponible en: https://auth0.com/blog/authentication-and-authorization-with-jwts-explained/

[11] Banafa A. The Evolution of Authentication and its Importance in Cybersecurity [Internet]. Analytics Insight; s.f. [citado 2023 Feb 17]. Disponible en: https://www.analyticsinsight.net/the-evolution-of-authentication-and-its-importance-in-cybersecurity/

[12] Kuppinger M. Continuous Authentication: ¿Why and How? [Internet]. KuppingerCole; s.f. [citado 2023 Feb 17]. Disponible en: https://www.kuppingercole.com/report/continuousauthentication

[13] Dropbox. ¿Qué es la autenticación de dos factores? [Internet]. Dropbox; s.f. [citado 2023 Feb 17]. Disponible en: https://experience.dropbox.com/es-la/resources/what-is-2fa

[14] SciELO - Scientific Electronic Library Online [Internet]. [place unknown]: SciELO; [date unknown] [cited 2023 Mar 4]. Available from: https://www.scielo.org/.

[15] Microsoft. ¿Qué es el phishing? [Internet]. [citado el 4 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing