Daniel Méndez Cruz1

1Centro de Investigación en Matemáticas-Unidad Zacatecas,  
Av. Universidad No.222, 98068, Zacatecas, México

{daniel.mendez}[@cimat.mx](mailto:daniel.mendez@cimat.mx,%20luis.julian@cimat.mx)

**Resumen**

**Actualmente las preocupaciones de seguridad de compañías como bancos, hospitales, gobierno, instituciones educativas, etc. Se han centrado en evitar riesgos de perdida de información. Por esta razón a menudo se utilizan sistemas basados en contraseñas de un solo uso para verificar la identidad de los usuarios. Sin embargo, dichas contraseñas vienen con grandes preocupaciones en cuestión de seguridad, ya que aún son incapaces de distinguir entre un usuario tratando de identificarse o un adversario (malware, hacker, ataques de fuerza bruta, etc.) que robó las credenciales. A menudo los usuarios utilizan contraseñas fáciles de adivinar, lo que da pauta a que los adversarios puedan obtenerlas y así comprometer la seguridad e integridad de la información que se encuentra contenida en los sistemas de información. Esto pone de manifiesto la necesidad de utilizar nuevos métodos tales como: autenticación segura basada en Tokens, autenticación basado en biométricos.**

1. **Introducción**

Los factores de la autenticación para los seres humanos se clasifican, generalmente en 3 casos: algo que el usuario es (ejemplo, la huella digital, patrón de retina), algo que el usuario tiene (ejemplo, tarjeta de identificación), algo que el usuario sabe (ejemplo, una contraseña, número de identificación personal). La combinación de estos métodos es utilizada a menudo para realizar autenticaciones más robustas.

Como bien es sabido hasta el momento el método más común es el mecanismo de autenticación basado en contraseñas [**2**].

El problema que tiene este método tan difundido en los sistemas de información es que, con el incremento de las cantidades de cuentas de usuarios, a estos se les dificulta recordarlos por lo que guardan sus credenciales en exploradores o aplicaciones, lo que reduce en gran medida la protección de las mismas.

Otra forma de lidiar con el inconveniente de la autenticación para el usuario, es mediante el uso de los mensajes de texto (**SMS**) que es un servicio muy popular en los teléfonos. El SMS es utilizado en aplicaciones de la vida diaria incluidas comercio móvil, banca electrónica, etc. [6]

Autenticación basada en Tokens es dada como una opción para elevar el factor de seguridad de las aplicaciones, ya que estos utilizan un dispositivo adicional que genera una clave, ya sea numérica o alfanumérica este tipo de autenticación también entra en la categoría de 2 factores [4].

El resto del artículo está organizado de la siguiente manera: sección 2 muestra características de los métodos de autenticación de dos factores, sección 3 ventajas y desventajas de la implementación de SMS, sección 4 principales características de la autenticación vía token.

1. **Métodos de Autenticación de 2 factores**

En 1991, Chang and Wu propusieron el primer esquema de autenticación remoto que combinaba Smart Cards y contraseñas para proteger servicios de seguridad critica.

La autenticación de dos factores o también conocido como (**2FA**) sube el listón hacia el atacante significativamente, sin embargo, aún es debatible si la tecnología puede ser adoptada de forma realista por la mayoría de los usuarios de internet. [7]

Una característica común de estos primeros esquemas de dos factores es que su seguridad en gran parte recae sobre la propiedad a prueba de falsificaciones de Smart Cards. [4]

La salvaje adopción de los servicios en línea por los usuarios de internet ha elevado sustancialmente la necesidad por una mejor autenticación. Ahora los usuarios requieren manejas hasta diez contraseñas distintas [7].

Otra de las practicas más utilizadas entre los usuarios es reciclar contraseñas que son utilizadas de servicio a servicio. El reciclar contraseñas puede traer consecuencias, cuando hay una pérdida de contraseñas. Por esta razón se han empezado a implementar medidas del lado del servidor para luchar contra el robo de contraseñas.

Se espera ver más servicios siendo desplegados en los próximos años. Además, vemos que Google, junto con Facebook y Yahoo, fueron de los primeros servicios que introdujeron un método de autenticación de 2 factores. La figura 1 nos muestra cada vez más la adopción de 2FA por varios proveedores de servicios a través de los años.

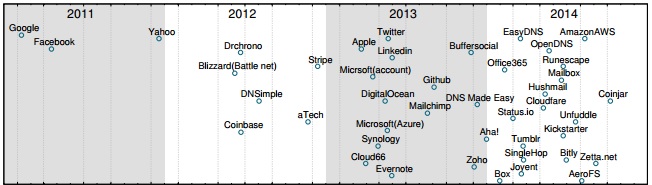


Figura 1: Adopción de 2FA por sitios y servicios web a través de los años [4].

La ventaja de utilizar el método de autenticación de 2 factores es que el usuario provee dos medios de identificación, uno es típicamente un token y otro es algo normalmente memorizado como alguna contraseña, se genera una secuencia aleatoria de 265 bits, está secuencia es enviada al token, y entonces utilizando una llave privada configurada en el dispositivo, el cual computa un algoritmo de cifrado con longitud variada, el cual permite verificar la integridad de los archivos a descifrar.

1. **Método de Autenticación vía SMS y sus contras**

SMS que significa Short Message Service, ha sido utilizado desde la era de las comunicaciones 2G, este representativo servicio es uno de los más utilizados servicios de teléfonos móviles. Una de las características del SMS es que es recibido en el teléfono móvil de usuario, lo cual lo convierte en un factor de autenticación basado en pertenencia [6].

A pesar de que el SMS no cuenta con los tres elementos de seguridad los cuales son confidencialidad, integridad, y disponibilidad, cuenta con su propio canal de comunicación. Es por esto que se utiliza como un servicio de autenticación en muchas áreas desde que el teléfono puede llevar a cabo acciones de autenticación basados en propiedad. Si es utilizado como servicio de autenticación en un sistema de entorno en internet, puede proveer un mayor medio de seguridad comparado con la autenticación de 1 factor [6].

Con el avance de la tecnología, los teléfonos móviles han cambiado de teléfonos con funciones a teléfonos inteligentes, así como también el sistema de comunicación cambio de 2G a 4G. Sin embargo, a pesar de estos avances, todavía sigue siendo un problema que un tipo de autenticación vía SMS insegura se utilice en muchas áreas, particularmente en los sistemas de pago que cuentan con autenticación y no repudio, lo cual lo convierte en un serio problema [10].

Dado a que se mencionan los problemas que se tiene al utilizar el método de autenticación vía SMS, ahora mostramos algunos puntos que pueden ser tomados en cuenta para proveer un servicio seguro.

En la tabla 1 se muestra algunos puntos importantes que pueden proveer un servicio de autenticación vía SMS seguro.

|  |  |
| --- | --- |
| Consideraciones | Descripciones |
| Confidencialidad | Para proveer la confidencialidad del mensaje de texto de autenticación, es necesario un canal seguro o el mensaje de texto debe de ser enviado y recibido en un formato cifrado. |
| Integridad | Para proveer la integridad del mensaje de texto, el hash y la firma deben de ser proporcionado. |
| Autenticación mutua | En cuanto a la autenticación mutua, se necesita agregar un paso para que el usuario se involucre directamente en la autenticación. |
| Algoritmo y longitud de clave | Algoritmo y la longitud de la clave deberán ser usados para el cifrado y firma de la autenticación del mensaje de texto. |
| Definición de pasos en el proceso de autenticación | Cada uno de los pasos del proceso de autenticación, incluido registro, verificación, etc. |

Tabla 1: consideraciones para una autenticación SMS segura [6].

1. **Autenticación vía Token**

A través de las pasadas décadas, las contraseñas como un medio de autenticación del usuario ha sido consecuentemente criticado por los mismos usuarios y analistas de seguridad por igual. A pesar de eso, los sistemas basados en contraseñas están atrincherados en la sociedad moderna, los usuarios están acostumbrados a utilizarlo, los administradores de sistemas están íntimamente familiarizados con su operación, así como los Frameworks que siguen generando contraseñas simples [4].

Bajo este enfoque de ofrecer alternativas confiables y facilitando el proceso de autenticación del usuario, así como descentralizar el método de autenticación de 1 factor, se crearon dispositivos electrónicos conocidos como tokens, los cuales tienen la finalidad de brindar al usuario un servicio autorizado que permite facilitar el proceso de autenticación hacia algún sistema [3].

Estos son utilizados para almacenar claves tales como firmas digitales, datos biométricos, etc. Existen muchos tipos de tokens, están los conocidos generadores de contraseñas dinámicas (**OTP**) y las que comúnmente se denominan token USB, permiten almacenar contraseñas y certificados, además de llevar la identidad del usuario.

Es por esto que el concepto de Tokens que se pretende es aplicado para proveer una manera para que los usuarios para autenticar cada solicitud sin tener la necesidad de mantener una sesión o mandar repetidamente las credenciales de login [9].

Un ejemplo de tokens puede ser dado por JSON web Token (**JWT**) es un medio estándar de la solicitud, en la cual codificada como un objeto JSON que es firmado y cifrado opcionalmente [9].

En este escenario se firma un JWT utilizando cifrado asimétrico, esto significa que los creadores del token necesitan una llave pública y privada. La llave pública necesita estar accesible para recibir el token, además la propiedad del nombre es asociada con la posesión de una correspondiente llave privada. El cliente utiliza la llave privada para generar un JWT auto firmado, desde que la contraseña es remplazada con una firma digital. Desde que la contraseña es remplazada por una firma digital, el esquema no involucra la creación de una cuenta en el servidor y el gestor de credenciales de usuario, así que incrementa el nivel el nivel de seguridad.

En la figura2 se muestra la implementación del esquema de autenticación utilizando JWT.

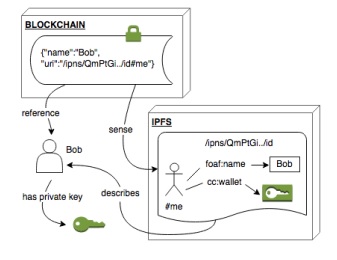


Figura 2: Patrón de interacción descentralizada JWT [9]

**Bibliografía:**

[1] Y. Bouzida and R. Beghdad, “Improving the timed token protocol,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2093, no. 213, pp. 520–529, 2001.

[2] S. Chandra, S. Paira, B. T. Student, S. Safikul, A. Assistant, and G. Sanyal, “A comparative survey of symmetric and asymmetric key cryptography,” *2014 Int. Conf. Electron. Commun. Compytational Eng.*, pp. 83–93, 2014.

[3] M. Chen and S. Chen, “An Efficient Anonymous Authentication Protocol for RFID Systems Using Dynamic Tokens,” *2015 IEEE 35th Int. Conf. Distrib. Comput. Syst.*, pp. 756–757, 2015.

[4] P. Crocker and P. Querido, “Two Factor Encryption in Cloud Storage Providers Using Hardware Tokens,” *2015 IEEE Globecom Work. (GC Wkshps)*, pp. 1–6, 2015.

[5] G. Fa and Q. Rogado, “Decentralized Semantic Identity.”

[6] J. Lee and Y. Oh, “A Study on Providing the Reliable and Secure SMS Authentication Service,” *2014 IEEE 11th Intl Conf Ubiquitous Intell. Comput. 2014 IEEE 11th Intl Conf Auton. Trust. Comput. 2014 IEEE 14th Intl Conf Scalable Comput. Commun. Its Assoc. Work.*, pp. 620–624, 2014.

[7] V. A. Pasenchuk and D. A. Volkov, “SignToLogin Cloud Service of Biometric Two-Factor Authentication Using Mobile Devices,” *17th Int. Conf. Micro/Nanotechnologies Electron Devices EDM*, pp. 164–167, 2016.

[8] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, “Two-factor authentication: is the world ready?,” *Proc. Eighth Eur. Work. Syst. Secur. - EuroSec ’15*, no. October, pp. 1–7, 2015.

[9] T. R., S. Y. R., S. H. Manjula, K. R. Venugopal, and L. M. Patnaik, “Token Based Privacy Preserving Access Control in Wireless Sensor Networks,” *2015 Int. Conf. Adv. Comput. Commun.*, pp. 45–50, 2015.

[10] M. Thomas, “Transmission of SMS,” 2015.

[11] D. Wang, Q. Gu, H. Cheng, and P. Wang, “The Request for Better Measurement,” *Proc. 11th ACM Asia Conf. Comput. Commun. Secur. - ASIA CCS ’16*, pp. 475–486, 2016.

[12] A. M. White, K. Shaw, F. Monrose, and E. Moreton, “Isn’t that Fantabulous,” *Proc. 2014 Work. New Secur. Paradig. Work. - NSPW ’14*, pp. 25–38, 2014.

[13] Z. Zhou, T. Zhang, S. S. M. Chow, Y. Zhang, and K. Zhang, “Efficient Authenticated Multi-Pattern Matching.,” *AsiaCCS*, pp. 593–604, 2016.

[14] J. Moon, J. Yu, H. Yang, and D. Won, “Improvement of Biometrics and Smart Cards-based Authentication Scheme for Multi-Server Environments,” *Proc. 10th Int. Conf. Ubiquitous Inf. Manag. Commun.*, p. 7:1--7:8, 2016.

[15] R. Gehlot, “Enhancing Security on Cloud using Additional Encrypted Parameter for Public Authentication,” pp. 0–4, 2016.

[16] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, “Robust multi-factor authentication for fragile communications,” *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 6, pp. 568–581, 2014.