Avances de la autenticación personal en el mundo digital y sus nuevas aplicaciones

Javier Leonardo Astaíza Castilla
javasca@gmail.com
Universidad Piloto de Colombia

Resumen. *En este documento se brinda información sobre los avances tecnológicos en el campo de la autenticación personal, buscando, a través de un compendio sobre los métodos actuales, dar una visión del contexto en el que se desarrollan estos avances y sus posibles aplicaciones y beneficios.*

Palabras clave: Métodos de identificación personal, biometría, ratón inteligente, seguridad informática, ondas cerebrales, verificación en dos pasos.

Abstract. *This document provides information on technological developments in the field of personal authentication, looking for, through a compendium of current methods, give an overview of the context in which these developments and their potential applications and benefits.*

Keywords: *Person authentication methods, biometric, smart mouse, information security, brainwaves, two step verification.*

I. APORTES REALIZADOS A LA INDUSTRIA TECNOLÓGICA A LO LARGO DE LA HISTORIA

La seguridad siempre ha sido importante a lo largo de la historia, son numerosas las contribuciones y desarrollos de varias personas y sectores de la industria que han permitido que nuestra seguridad física y “no física” (podemos llamar así a aquella que está relacionada con todo lo sujeto a nuestra identidad, posesiones, bienes, documentos y en la actualidad, nuestro yo digital) evolucione.
Es imperiosa la necesidad actual de asegurar también en el mundo digital, que toda la información que es nuestra, que nos identifica, es gestionada únicamente por nosotros mismos y que somos únicamente nosotros quienes actuamos en este mundo de “personajes invisibles”.

Hay una industria que lejos de ser ajena a estos avances en seguridad, ha sido promotora de grandes desarrollos exclusivos para su sector, pero que la sociedad y otros sectores industriales al ver el gran potencial de los mismos, los grandes beneficios que podía otorgar a la población, evidenció la necesidad de masificar estos logros.

Me estoy refiriendo a la industria militar, que en momentos de

conflicto y paz, se ha visto impulsada a crear soluciones que permitan superar a sus rivales, que lleven a sus naciones a liderar el avance e innovación tecnológica, determinante para vencer.

Muchos de estos logros en la industria militar los vemos hoy implementados para uso civil, para nuestro uso, para beneficio de la humanidad. Es el caso de la radio, la comida enlatada, el horno microondas, el sistema de posicionamiento global (GPS), y sin ir más lejos, uno que ha hecho revolucionar al mundo y nuestra forma de desempeñarnos en él: Internet, que surgió de la necesidad de satisfacer un requerimiento del Departamento de Defensa de Estados Unidos.

Como se mencionaba en líneas anteriores, desarrollos que en su momento fueron exclusivamente para uso militar, pero que era innegable el gran provecho, incluso económico, que se iba a generar al entregarlo a otros sectores.

II. AVANCES LOGRADOS EN LOS MÉTODOS DE AUTENTICACIÓN PERSONAL

Es por esto que en este documento realizaré un análisis del artículo "*Smart gun inspires smart mouse*" [1], que se publicó en la página de internet http://www.computerworld.com/, y que trata acerca de un nuevo método para autenticar a los usuarios de un sistema a través de un ratón inteligente.

En este caso la industria militar inspira de nuevo este avance en seguridad. Hace unos años, se desarrolló un método para autenticar a la persona que iba a hacer uso de un arma de fuego por medio de sensores de presión, en caso de no ser el usuario autorizado, no se podría disparar el arma.

Precisamente sobre esto se informó el ingeniero en ciberseguridad Glenn Kaufman de la empresa estadounidense Raytheon y alimentó así su inquietud para desarrollar un método similar para autenticar al usuario de un ratón. Recientemente se ha otorgado la patente al señor Kaufman por este desarrollo [2],[3],[4].

Podríamos decir que este método de autenticación cabe dentro del grupo de identificación biométrica, pero si vamos un poco más al detalle, es una identificación neuronal, ya que dependiendo de cómo manipulemos el dispositivo, la fuerza ejercida sobre él, se determinará si efectivamente es el usuario autorizado para tener acceso.

III. ESTADO ACTUAL DE LOS MÉTODOS DE AUTENTICACIÓN EN EL MUNDO DIGITAL

Antes de continuar dando detalles sobre este avance, considero pertinente comentar un poco sobre los tipos de métodos de autenticación personal que encontramos en la actualidad, y así poder tener un contexto más claro sobre la diferencia y aporte que brinda este nuevo desarrollo.

Los actuales sistemas de autenticación personal se pueden reunir en tres grandes grupos o factores, aquellos basados en el *conocimiento*, los que se basan en la *posesión* y los que recurren a validar lo que *nosotros somos*, es decir, nuestras características físicas, pensamientos, etc. en otras palabras, todo aquello que es *inherente* a nosotros.

En los sistemas de identificación basados en conocimiento, encontramos el uso de las contraseñas: numéricas en el caso de los cajeros electrónicos, alfanuméricas en casi todos los dispositivos hardware y software, y los patrones, generalmente de imagen.

Un tipo de verificación que es práctico, debido a que es fácil de recordar. Precisamente nosotros como usuarios al desear un ingreso sencillo cometemos el error de crear contraseñas fáciles, que no impliquen un mayor esfuerzo para memorizarlas, hacemos uso de palabras del diccionario, de cosas muy familiares para nosotros, es ahí cuando empieza a hacerse débil este método.

La ingeniería social, el contacto con personas que nos conocen y sistemas que realizan ataques de fuerza bruta pueden llevar a descubrir fácilmente algo que, inicialmente, creemos que solo nosotros conocemos.

Los sistemas basados en posesión, como su nombre lo indica, dependen de algo que esté en nuestro poder, por lo general algo físico. Es así como encontramos en este momento, tokens (dispositivos que generan valores numéricos, alfanuméricos), dispositivos móviles: celulares, etc. y en otros casos se hace uso de archivos que confirman nuestra identidad ante un sistema.

Estos sistemas basan su seguridad en el supuesto que solo nosotros tenemos acceso a estos elementos y que alguien que desee suplantarnos debe lograr tenerlos.

Los sistemas basados en lo que es inherente a nosotros, y aquí podemos mencionar que es prácticamente la manera como nos identificamos en el mundo real, a través de nuestro rostro, nuestra voz, etc. En esta categoría podemos incluir todos los tipos de identificación biométrica: reconocimiento de retina, reconocimiento de patrones de huella digital,

reconocimiento facial, etc. Podríamos decir que con este tipo de autenticación estamos tratando de darle la capacidad a las máquinas y a los sistemas de reconocernos como lo hacemos nosotros con nuestros semejantes.

Y como sucede en este caso de estudio, la tecnología da un paso más agregando los avances en identificación neurológica a estos sistemas de autenticación.

Desafortunadamente los métodos incluidos en estos tres grupos por sí solos no pueden garantizar de manera fidedigna que la persona que dice ser, sea.

Es por esto que es necesario tomar las fortalezas de cada uno ellos y usarlos combinadamente para obtener mejores resultados. A este proceso se le denomina *autenticación multifactor*.

Muchos servicios digitales en la actualidad hacen uso de esto para brindar una mejor seguridad, un ejemplo es la verificación en dos pasos de plataformas como Gmail, Outlook, que hacen uso de dos factores, conocimiento y posesión (la combinación más frecuente) para dar acceso al sistema, específicamente solicitando una contraseña y un valor numérico que puede ser entregado vía mensaje de texto a un celular (SMS) o por medio de una aplicación que genera este mismo código en el mismo teléfono.

Esto otorga un nivel más de seguridad al garantizar que si han descubierto nuestra contraseña no pueden ingresar a la cuenta a menos que el atacante también tenga en su poder nuestro teléfono.

¿Qué sucede si no tenemos nuestro teléfono con nosotros? Sencillamente otra opción de posesión, se nos dará un listado de códigos que podemos imprimir o copiar en alguna parte, obviamente partiendo de la idea inicial, en la que se asume que sólo nosotros podemos tener acceso a estos códigos.

IV. ANÁLISIS DE LOS DESARROLLOS ACTUALES

Después de este breve resumen sobre los métodos de autenticación existentes, podemos continuar con el estudio y desarrollo realizado por el señor Kaufman.

¿Era posible por medio de sensores de presión en la empuñadura de un arma generar resultados que al analizarlos permitieran identificar a un usuario de un dispositivo periférico, como un ratón?

El ingeniero construyó el dispositivo al que dotó de sensores de presión y al realizar las pruebas confirmó que al igual que en el arma, la forma en que las personas tomaban el ratón difería entre cada uno de los

participantes.

En palabras de Kaufman: “No es sólo la cantidad de presión que se ejerce en el propio ratón, sino también las coordenadas *xy* de su posición" [1]. A esto podemos añadir: “Son sus nervios y el nervio que controla sus músculos el que produce esta firma” [1].

Estas afirmaciones del creador del ratón inteligente nos demuestran que este acto es único en cada persona, de forma tal que la autenticación se logra creando un número neurológico que surge de las diversas lecturas generadas por los sensores de presión y comparándolo con un número neurológico registrado, si el número concuerda se permite el acceso al sistema en el cual está acoplado el dispositivo.

Este notable desarrollo en los métodos de identificación biométrica no lo hace mutuamente excluyente de los anteriormente mencionados, al contrario, su función es la de complementarlos, de hacer más difícil la suplantación de un individuo, de ser “sólo una capa adicional para, básicamente, autenticarse en el sistema” [1].

Tenemos pues, un ingrediente más en nuestra receta de los métodos de identificación personal, para que a gusto de las organizaciones, industrias, desarrolladores y usuarios, se mezclen en pro de la seguridad en el mundo digital.

Antes de brindar una reflexión final sobre lo que se ha comentado, quiero hacer una breve mención de otro estudio que se ha realizado, basado en un experimento para autenticar usuarios mediante el uso de sus ondas cerebrales [4]. Esto se logró por medio de sensores de electroencefalogramas en audífonos inalámbricos y otra serie de productos comerciales.

La clave de este método se basa en nuestros pensamientos, es decir en crear una contraseña o “pass-thoughts” a partir de la evocación recurrente de algún recuerdo (recitar un texto, cantar una canción sin emitir ruido), alguna actividad física (simular el movimiento de los dedos, imaginar el movimiento que se debe realizar para practicar algún deporte) u otro tipo de tarea mental que se ha establecido previamente.

En el estudio se menciona que quizás donde los otros métodos de autenticación han fallado, este puede tener éxito, y es en el *balance entre seguridad y facilidad de uso.* Esta autenticación neuronal puede convertirse en el método más seguro y no implica mayores desafíos para nosotros como usuarios. ¿Alguien más puede tener acceso a nuestros pensamientos?, hasta el momento la respuesta parece ser negativa.

En los sistemas de autenticación basados en conocimiento se

hace complejo recordar una cadena cada vez más larga de caracteres para cada servicio utilizado considerando que recordar una imagen, un rostro, es mucho más sencillo (lo hemos hecho durante toda nuestra vida) y con una ventaja adicional, pueden pasar periodos de tiempo largos, semanas o meses y estos recuerdos difícilmente pueden borrarse.

V. UN VISTAZO AL FUTURO

Es grato imaginar todas las posibles aplicaciones que se podrán generar con estas invenciones y que llevarán a grandes cambios en la forma en que interactuamos con las cosas.

Muchos de estos estudios nos impulsarán, sin duda, a tener en un tiempo accesos más sencillos, e incluso naturales, a los dispositivos con los que interactuamos todos los días, teléfonos celulares, computadores, automóviles (quizás la doble autenticación que ya existe para el ingreso a algunos de ellos combinando el factor de conocimiento, un código de alarma, y posesión, una llave, migre hacia la identificación biométrica que nos propone el arma o el ratón inteligente), que nuestra nevera, televisor, etc. permita su operación sólo hasta que se haya autenticado al usuario que desea usarlo.

VI. CONCLUSIONES

Es necesario resaltar que estos avances quizás tarden un poco en llegar a nuestras manos, pero es tarea nuestra, las personas vinculadas a la industria de la tecnología o sencillamente como usuarios, estar al tanto de la información concerniente a ellos y propender a la masificación y uso de los mismos.

Aunque son evidentes las grandes ventajas de los avances que se han logrado, y mientras estamos en esa espera activa para que estén al alcance de todos nosotros, no podemos dejar de lado lo que la tecnología nos brinda hoy. Tenemos que indagar más sobre lo que someramente se trató en párrafos previos, acerca de los métodos de autenticación que nos brindan las plataformas que usamos actualmente, por ejemplo, plataformas de correo electrónico, redes sociales, banca personal y empresarial, comercio electrónico, aplicaciones para dispositivos móviles.

Muchos de estos servicios, actualmente ofrecen estas mejoras relacionadas con la autenticación, pero es necesario que seamos un poco curiosos, tomarnos el tiempo para realizar las modificaciones necesarias a las configuraciones preestablecidas (generalmente poco seguras), y lograr así que nuestra información pueda estar más segura. Aunque no todo depende de nosotros, sí somos

parte importante de esta cadena de la seguridad de la información en el mundo digital, y colocando nuestro grano de arena al seguir estas recomendaciones, podremos estar más confiados que sólo nosotros, los dueños de esa información, somos quienes la manipulamos.

Podemos convertirnos en agentes de cambio por medio de nuestros trabajos, al proponer en nuestras organizaciones formas de aplicar a nuestros productos y/o servicios, evoluciones como las que han sido mencionadas.

Podemos, sin duda, ser también agentes de cambio al motivar y explicar a nuestros familiares, amigos y conocidos (quienes probablemente no tienen el conocimiento o inquietud suficiente), el uso de todas aquellas prácticas que permitan lograr un mundo físico y virtual más seguro.

REFERENCIAS

[1] P. Thibodeau. (2014, Octubre 3). “Smart gun inspires smart mouse. A new method for authenticating users via a mouse wins patent.” Disponible en: http://www.computerworld.com/article/2691597/smart-gun-inspires-smart-mouse.html

[2] G. R. Kaufman, “Biometric pressure grip”, U.S. Patent 8762734 B2, Junio 24, 2014. Disponible en: http://www.google.com/patents/US8762734

[3] G. R. Kaufman, “Biometric pressure grip”, U.S. Patent 8762734 B2, Junio 24, 2014. Disponible en: http://www.uspto.gov/web/patents/patog/week25/OG/html/1403-4/US08762734-20140624.html

[4] J. Chuang, H. Nguyen, C. Wang, B. Johnson. “I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves”. Disponible en: http://people.ischool.berkeley.edu/~chuang/pubs/usec13.pdf

Autor

Javier L. Astaíza C.

Ingeniero de sistemas, estudiante de la especialización en seguridad informática de la Universidad Piloto de Colombia, certificado ITIL Foundation in IT Service Management.

Experiencia en gestión de infraestructura tecnológica, administración de redes y servidores Windows, desarrollo de sistemas de gestión de seguridad de la información basado en la norma ISO 27001.