DISPOSITIVOS BIOMÉTRICOS PARA SEGURIDAD

Crisel Nohelia Haro Antonio
haroantoniocrisel3f@gmail.com
Luis Arturo Mora Flores
lamf99@icloud.com
Claudia Marina Vicario Solorzano
marina.vicario@gmail.com

Instituto Politécnico Nacional
Unidad Profesional Interdisciplinaria de Ingeniería,
Ciencias Social y Administrativas.

Resumen

El aumento sistemático de la digitalización de los datos ha generado un nuevo conflicto para su protección, por lo menos más de una tercera parte de la población ha pasado por los problemas de robo de identidad, robo de cuentas bancarias e información médica, pero los dispositivos biométricos ayudarán a ir superando esa barrera de inseguridad, no solo con las huellas dactilares sino con la utilización del patrón de venas. Por ello se quiere describir las ventajas y desventajas en este trabajo para lograr ver qué tan beneficiosa es la seguridad con datos biométricos, que aún no están exentos de suplantación pero tienen un grado mayor de protección porque es difícil lograr copiar esos datos fisiológicos.

Palabras Clave: Ciberseguridad, dispositivos biométricos, reconocimiento de huellas digitales, detección de ataques de presentación, seguridad.

Abstract

The systematic increase in the digitization of data has generated a new conflict for its protection, at least more than a third of the population has gone through the problems of identity theft, theft of bank accounts and medical information, but the devices Biometrics will help to overcome this barrier of insecurity, not only with fingerprints but with the use of the vein pattern. For this reason, we want to describe the advantages and disadvantages in this work to see how beneficial is security with biometric data, which are not yet exempt from impersonation but have a higher degree of protection because it is difficult to copy these physiological data.

Keywords: Cybersecurity, biometric devices, fingerprint recognition, presentation attack detection, security.

Introducción

Alguna vez, ¿has pensado si tu información está segura? Pues en muchos casos no sabes qué tan vulnerable se encuentra, pero hay países que ya empiezan a notar su importancia. “Suecia obtiene regularmente los mejores resultados cuando se evalúa a los países en términos de madurez digital y TIC.” (Franke, 2017, p. 131) Suecia invierte en ciberseguridad, pero sería mejor ahorrar toda esa inversión si contáramos con dispositivos biométricos que nos facilitaran la autenticación de nuestra identidad. “El mercado sueco de ciberseguridad está creciendo rápidamente, pero el seguro cibernético en Suecia actualmente es adquirido principalmente por grandes empresas.” (Franke, 2017, p. 142) Esto deja de lado a los ciudadanos, ya que estos seguros tienen un alto costo.

También está la utilización de la tecnología blockchain. “Los principales hallazgos de la revisión del alcance muestran que hasta ahora se ha propuesto la tecnología blockchain para abordar varios problemas de seguridad en una serie de diferentes aplicaciones biomédicas…” (Drosatos & Kaldoudi, 2019, p. 237) y aunque este autor se enfoque en la seguridad de las aplicaciones biomédicas, también ayudarían a otras áreas, pero esta aún se encuentra en desarrollo por lo que sería más conveniente la utilización de dispositivos biométricos.

Figura 1.1 Dispositivos biométricos
Fuente: Pérez, O. (2019). Recuperado de http://www.cubadebate.cu/opinion/2019/11/07/hablando-de-ciberseguridad-xii/?utm-source=dlvr.i&utm_medium=twitter#.XvDasJpKjIU

Pero en la actualidad, la mayoría de la población tiene un dispositivo inteligente el cuál te permite desbloquear con tu huella dactilar, que también sirve como autenticador de identidad si se aplicará en los demás sectores.

Entonces estos datos físicos que componen los datos biométricos hacen más fácil la protección de sus datos, ya que no necesitan un token o una contraseña memorizada, y sí, como todo sistema también tienen una vulnerabilidad por los ataques externos, el dispositivo de captura biométrica es probablemente el más expuesto ya que un atacante eventual no requiere conocimiento sobre el funcionamiento interno del sistema para romper el mismo.

En cambio, uno simplemente puede presentar el dispositivo de captura con un instrumento de ataque de presentación (PAI), como un dedo gomoso o una superposición de huellas digitales, para interferir con su comportamiento previsto.

El objetivo principal podría ser hacerse pasar por otra persona (es decir, un impostor activo) o evitar ser reconocido (es decir, un ocultador de identidad). Estos ataques son conocidos en ISO / IEC 30107 como ataques de presentación (AP), además de tener la desventaja del tiempo, ya que nuestros rasgos cambian y se van perdiendo, entonces estos ya no serían reconocidos por los dispositivos biométricos.

Sin embargo, la implementación adecuada de estos dispositivos en empresas, bancos, compras por internet, etc., Significaría una mayor seguridad para los datos de cada persona que ha sufrido por estos impostores activos.

Desarrollo:

1. Datos Biométricos

Los datos biométricos son aquellas características biológicas que nos distingue como individuos, por ejemplo, las huellas dactilares, el patrón de la vena, la forma de la cara, el iris, la retina, incluso algunas características del comportamiento como la voz, la presión sobre las teclas, los gestos. Estos rasgos nos hacen individuos únicos y entonces estos rasgos cómo se podrían aplicar a la seguridad de nuestra información, sin la necesidad de un tokens, tarjetas magnéticas o memorización de contraseñas para vincular nuestras identidades (Douglas, Bailey, Leeney y Curran, 2017).

Aunque en la actualidad las personas no tienen una conciencia de lo que realmente significa el robo de identidad o información personal de cualquier índole debido a una baja cultura de seguridad y esto es en verdad un reto (Ki-Aries & Faily, 2017). Y realmente representa un verdadero reto porque se necesita de una estructura para empezar a enseñar sobre esta práctica, si bien algunas empresas gubernamentales hacen publicidad sobre el uso de sus datos personales, realmente, ¿Los individuos entienden de lo que se está hablando? Generalmente vivimos en una sociedad donde la gente adulta es la que lidera la población y muchas de ellas no son conscientes del uso de su información en la red o si alguna vez ha sido violada.

Y solo por mencionar que los delitos de robo de identidad, financieros e incluso médicos en los Estados Unidos ha superado los 2 mil millones de personas afectadas, teniendo como principales afectadas a las mujeres, que incluso no solo es el robo de identidad sino la extorsión para la recuperación de esa información (Poster, 2018).

Y esto se debe principalmente a que en los últimos años, por la evolución de la tecnología y la necesidad de acceder de manera más rápida a la información, el volumen de datos y procesos en las plataformas de la nube hayan crecido, es por ello que se han generado estas amenazas de seguridad en la privacidad, confidencialidad e integridad de los datos, que aún se combate y no tienen una solución específica, aunque más adelante hablaremos sobre estas medidas (Gomez, Galbally, Morales & Fierrez, 2017).

En el presente la mayoría de las personas, sino es que todas hemos visto los más recientes smartphones, que ahora cuentan con lectores de huella que nos permiten desbloquear el dispositivo. Entonces este mismo método no solo se podría aplicar solo para la seguridad de los smartphones, sino también para la seguridad de las bases de datos financieras, médicas o de cualquier índole que necesite un nivel de seguridad, y esto debe ser una realidad por la demanda de la sociedad ante la necesidad de la autenticación automática y confiable, es por ello que se que han empezado a implementar sistemas biométricos, principalmente en iniciativas internacionales (Tolosan, Gomez, Busch & Ortega, 2010).

Figura 1.2 Huella digital.
Fuente: Martínez, V. (2019). Recuperado de https://www.elmundo.cr/costa-rica/hospital-de-geriatria-estreno-uso-de-huella-dactilar/

Este sistema tiene muchas aplicaciones, desde el control fronterizo hasta servicios financieros, es sin duda alguna la principal ventaja que haría que se desplazarán los tokens o contraseñas tradicionales (Söllinger, Trung & Uhl, 2018). Sin embargo, también es preciso tener un protocoló para la gestión de este sistema (Höglunda, Lindemera, Furuhedb & Razaa, 2020). Además de pensar en que estos sistemas de autentificación y seguridad de la información necesitarán de un buen hardware que no limite sus funciones (Pan, Li, Zhang & Weng, 2018).

2. Ventajas y Desventajas

Si bien estos dispositivos nos generarían una enorme ayuda para la seguridad también cuenta con ciertos errores que no garantizarían su funcionalidad al cien por ciento, algunos casos son los siguientes: los dispositivos sensores que registrarían la información en primer lugar pueden tener una mala calidad haciendo inútiles los datos, esto se da principalmente por la mala calidad de los enlaces de comunicación inalámbrica (Kos & Kramberger, 2017). Además de contar con los ataques externos como introducción de datos fraudulentos, esto nos dice que se pueden llevar a cabo mediante artefactos que imitan rasgos biométricos de otras personas para engañar al sistema (Söllinger et al., 2018).

De hecho, estás prácticas se han hecho más comunes, causando la necesidad de crear software que detectan el comportamiento de estos malware. “Se ha convertido en una herramienta común en robo digital, espionaje corporativo y nacional, distribución de spam y ataques a la disponibilidad de infraestructura.” (Wagnerab, Rindab, Thüra & Aignerab, 2017, p. 1).

Estos dispositivos biométricos principalmente se enfocarían en el área empresarial, financiera y médica, por la parte del hardware capacitado para una total funcionalidad del software, y no solo se haría el reconocimiento por medio de huellas dactilares, sino con el patrón de venas de la mano. Y aunque estas representen una mayor ventaja contra el robo de identidad, ahora el tiempo será nuestro mayor enemigo, ya que el cambio fisiológico con el tiempo hace estos rasgos inutilizables para identificar

automáticamente a las personas, esto refiriéndonos a las huellas dactilares y forma del rostro, en cambio el patrón de venas no presenta un cambio significativo, pero sí una mayor inversión para el hardware necesario para la recopilación de información. (Tolosan et al., 2010).

Conclusiones

Recalcamos la importancia del uso de estos dispositivos, para tener una mayor seguridad de nuestra información, claro que aún se necesitan cubrir todas las variables sueltas con respecto a la eficiencia del hardware pero se está intentando.

El proyecto internacional Beacon fue diseñado como un servicio web público para permitir a las instituciones compartir información resumida sobre los repositorios de datos genómicos. Específicamente, Beacon permite a los usuarios consultar la existencia de cualquier genoma dadas las entradas de consulta como variante, posición y cromosoma. Actualmente, hay más de 200 programas involucrados que contribuyen a la Red Beacon. Sin embargo, Shringarpure y Bustamante (SB) demostraron que, en las circunstancias correctas, un usuario malintencionado podía identificar la presencia de un individuo detrás de una baliza mediante consultas repetidas de las variantes genómicas del individuo.

(Wang, S., Jiang, X., Tang, H., Wang, X., Bu, D., Carey, K., OM Dyke, S., Fox, D., Jiang, C., Lauter, K., Malin, B., Sofia, H., Telenti, A., Wang, L., Wang, W. & Ohno-Machado, L., 2017).

Dados estos ejemplos nos podemos dar cuenta de cómo la protección de datos en el sector médico es y ha sido de suma importancia, ya que el robo de datos es un delito muy grave y en este sector puede resultar algo catastrófico si cae en manos equivocadas por el mal uso que se les pueden dar, por eso mismo se han creado estos programas y proyectos con la finalidad de mejorar esta problemática que se tiene hoy en día.

Sin embargo, aún hay detalles que se pueden seguir mejorando en estos proyectos para así evitar el robo de datos genómicos, esto se puede mejorar con la tecnología que existe hoy en día ya que sabemos que no es suficiente con un lector de huella o un lector de cara o hasta con lector de retina, ya que estos se han visto vulnerados por usuarios malintencionados.

Referencias

1. Wang, S., Jiang, X., Tang, H., Wang, X., Bu, D., Carey, K., OM Dyke, S., Fox, D., Jiang, C., Lauter, K., Malin, B., Sofia, H., Telenti, A., Wang, L., Wang, W. & Ohno-Machado, L. (**2017, octubre 27**).*A community effort to protect genomic data sharing, collaboration and outsourcing.Nature Communications,*Volumen 2, 1-6. 2020, febrero 21, De
   Scopus Base de datos.

2. Wagnerab, M., Rindab, A., Thüra, N. & Aignerab, W. (**2017, Junio**). *A knowledge-assisted visual malware analysis system: Design, validation, and reflection of KAMAS. Computers & Security*Volume 67, 1-15. 2020, Febrero 20, De
   Scopus Base de datos.

3. Galbally, J., Haraksim, R. & Beslay, L. (**2018, octubre 25**). *A Study of Age and Ageing in Fingerprint Biometrics. IEEE Transactions on Information Forensics and Security,*Volumen 14, 1351 - 1365. 2020, febrero 21, De
   Scopus Base de datos.

4. Kos, M. & Kramberger, I. (**2017, marzo 1**). *A Wearable Device and System for Movement and Biometric Data Acquisition for Sports Applications.Acceso IEEE,*Volumen 14, 1351 - 1365. 2020, febrero 21, De
   Scopus Base de datos.

5. Douglas, M., Bailey, K., Leeney, M. & Curran, K. (**2017, noviembre 29**). *An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applica-*

*tions,*Volumen 77, 17333 - 17373. 2020, febrero 21, De
Scopus Base de datos.

6. Tolosana, R., Gomez, M., Busch, C. & Ortega, J. (**2010, agosto 12**). *Biometric Presentation Attack Detection: Beyond the Visible Spectrum. IEEE Transactions on Information Forensics and Security*Volumen 15, 1261 - 1275. 2020, febrero 21, De
Scopus Base de datos.

7. Drosatos, G. & Kaldoudi, E. (**2019, febrero 8**). *Blockchain Applications in the Biomedical Domain: A Scoping Review. Computational and Structural Biotechnology Journal*volume 17, 229 - 240. 2020, febrero 20, De
Scorpus Base de datos.

8. Poster W. R. (**2018, marzo 26**). *Cybersecurity needs women. Nature Communications* 2020, febrero 21, de
Sitio web: https://www.nature.com/articles/d41586-018-03327-w

9. Söllinger, D., Trung, P. & Uhl, A. (**2018, julio 1**). *Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing.IET Biometrics,*Volumen 7, 314-324. 2020, febrero 21, De
Scopus Base de datos.

10. Ki-Aries, D. & Faily, S. (**2017, septiembre**). *Persona-centred information security awareness.Computers & Security*Volume 70, 663-674. 2020, febrero 20, De
Scopus Base de datos.

11. Alvez, C., Benedetto, M., Etchart, G., Luna, L., Leal, C., Fernández, M., Berón, G., & Loggio, S. (**2014**). *PID 7035 Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales.Ciencia, Docencia Tecnología Suplemento*4(4), 48-71. Recuperado a partir de
http://www.pcient.uner.edu.ar/Scdyt/article/view/7

12. Höglunda, J., Lindemera, S., Furuhedb, M.& Razaa, S. (**2020, febrero**). *PKI4IoT: Towards public key infrastructure for the Internet of Things.Computers & Security*Volume 89, 1-11. 2020, febrero 20, De
Scopus Base de datos.

13. Gomez, M., Galbally, J., Morales, A. & Fierrez, J. (**2017, abril 27**). *Privacy-Preserving Comparison of Variable-Length Data With Application to Biometric Template Protection.IEEE Access*Volumen 5, 8606 - 8619. 2020, febrero 21, De
Scopus Base de datos.

14. Yie-Teh, H., Kempa-Liehr, A. W. & I-Kai, K. (**2020, febrero 11**). *Sensor data quality: a systematic review.Journal of Big Data,*Volume 7, 1-49. 2020, Febrero 20, De
Scopus Base de datos.

15. Franke, U. (**2017, Julio**). *The cyber insurance market in Sweden.Computers & Security*Volume 68, 130-144. 2020, febrero 20, De
Scopus Base de datos.

16. Pan,W., Li, Z., Zhang, Y. & Weng, C. (**2018, septiembre 24**). *The New Hardware Development Trend and the Challenges in Data Management and Analysis. Data Science and Engineering*Volume 3, 263–276. 2020, febrero 20, De
Scopus Base de datos.

17. Pérez, O. (**2019, septiembre 23**). *Hablando de ciberseguridad (XII) [Figura]libro,revista o nombre de la página web*Recuperado de http://www.cubadebate.cu/opinion/2019/11/07/hablando-de-ciberseguridad-xii/?utm-source=dlvr.i&utm_medium=twitter#.XvDasJpKjIU

18. Martínez, V. (**2019, noviembre 7**). *Hospital de Geriatría estrenó uso de huella dactilar [Figura]. libro,revista o nombre de la página web*texto restante https://www.elmundo.cr/costa-rica/hospital-de-geriatria-estreno-uso-de-huella-dactilar/