Estudio de vulnerabilidades en mecanismos de autenticación para el control de acceso en instalaciones industriales – Dislicores S.A.S

Autores

Juan Esteban Puerta Cano

Asesores

Juan Camilo Giraldo

Maestría en Gestión de la información
Facultad de ingenierías
tecnológico de Antioquía

Resumen

Para las organizaciones es de gran importancia tener y brindar entornos seguros, donde toman fuerza los sistemas basados en reconocimiento biométrico, ya que pueden restringir accesos e identificar al personal. Comparado con otros métodos como llaves o claves, los rasgos biométricos no pueden en general, ser prestados, robados o copiados [1].

"Los rasgos biométricos pueden clasificarse a partir de varias características, entre ellas cabe mencionar su unicidad, su distintividad o individualidad, su universalidad, su facilidad de proceso y adquisición o su variabilidad con el tiempo. La huella dactilar reúne muchas de estas características y por ello ha sido muy utilizada tradicionalmente en el ámbito forense y más recientemente en los sistemas de autenticación automática "[2].

El presente trabajo presenta un estudio sobre las vulnerabilidades en mecanismos de control de acceso con dispositivos biométricos de autenticación por huella dactilar. Se tomará como caso para aplicar los resultados del estudio, la implementación de un escenario, donde se evaluará la arquitectura, y la aplicación de los dispositivos utilizados en la compañía Dislicores S.A.S. El estudio se basa en la información requerida para obtener los resultados de las posibles vulnerabilidades existentes en los dispositivos biométricos de la organización, mediante estudios de campo y experimentos.

La investigación toma relevancia, al presentar la información de posibles vulnerabilidades y amenazas que tienen los dispositivos biométricos y que no se han tenido en cuenta dentro del plan de seguridad de la información de la compañía.

Palabras Clave: Biometría, *Software*, *Hardware*, Vulnerabilidades, Amenazas, Huella Dactilar, Identidad, Control de acceso biométrico, Plantilla, Encriptación.

Abstract

For organizations, it is of great importance to have and provide safe environments, where systems based on biometric recognition gain strength, since they can restrict access and identify personnel. Compared to other methods such as keys or passwords, biometric features cannot generally be borrowed, stolen or copied [1].

“Biometric traits can be classified based on several characteristics, including their uniqueness, their distinctiveness or individuality, their universality, their ease of processing and acquisition, or their variability over time. The fingerprint has many of these characteristics and for this reason it has been widely used traditionally in the forensic field and more recently in automatic authentication systems "[2].

This work presents a study on vulnerabilities in access control mechanisms with biometric fingerprint authentication devices. It will be taken as a case to apply the results of the study, the implementation of a scenario, where the architecture is evaluated, and the application of the devices used in the company Dislicores S.A.S.
The study is based on the information required to obtain the results of the possible vulnerabilities existing in the biometric devices of the organization, through field studies and experiments.

The investigation becomes relevant, by presenting information on possible vulnerabilities and threats that biometric devices have and that have not been taken into account within the company's information security plan.

Key Words: Biometrics, *Software*, *Hardware*, Vulnerabilities, Threats, Fingerprint, Identity, Biometric access control.

Bibliografía

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[3] A. K. Jain, A. Ross, and U. Uludag, “Biometric template security: Challengesand solutions,” Proc. of 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey, 2005.

[4] Jean-Marc Royer “Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones” (2007) Ediciones ENI

[5] Cortés Osorio Jimy Alexander, Media Aguirre Francisco Alejandro, Muriel Escobar José “Sistemas de Seguridad basados en Biometría”, 2010.

[6] Diaz Martinez Marcos “Vulnerabilidades en sistemas de reconocimiento basados en huella dactilar: Ataques Hill-Climbing” (2008).

[7] Puerta C. Juan Esteban – Gomez Carlos, “Ataques informáticos al Interior de las Organizaciones” (2018).

[8] Peltier, “Control de Acceso”(2014).

[9] J. Ortega García, F. Alonso Fernandez y R. Belmonte Coomonte, Biometría y Seguridad, Madrid, España: Fundación Rogelio Segovia, 2008.

[10] A. Giraldo y D. Gómez, «Estado del Arte de la Seguridad en Sistemas Biométricos,» Bogotá, (2017).

[11] Murillo-Escobar M.A.∗ Cruz-Hernández C. Abundiz-Pérez F. López-Gutiérrez R.M. “Cifrado caótico de plantilla de huella dactilar en sistemas biométricos” (2014)

[12] Mg. Luzmila Pró1, Mg. Juan Carlos Gonzáles1, Lic. Walter Contreras1, Lic. Carlos Yañez1 “Tecnologías Biométricas aplicadas a la seguridad en las organizaciones” (2015).

[13] Ximena Vanessa Tapia Jaramillo “Revisión Sistemática de Literatura: Vulnerabilidad de sistemas biométricos basados en huellas dactilares” (2017).

[14] Marcos Faúndez Zanuy "Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos" (2010).

[15] Cañón Oscar Iván, Cuellar Castro Alonso "Sistemas de acceso y control para la gestión documental por sistemas de reconocimiento biométrico (Huella dactilar e iris)" (2018).

[16] Giraldo Girado Andrés, Gómez Ramírez Diana Patricia "Estado del arte de la seguridad en sistemas biométricos" (2017).

[17] Guerrero Erazo Henry Aldemar, Lasso Garcés Lorena Alexandra, Legarda Muñoz Paola Alexandra "Identificación de Vulnerabilidades de seguridad en el control de acceso al Sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S" (2015).

[18] Shsconsultores," La evaluación de la seguridad en sistemas biométricos" (2018).

[19]P, León, Susan K, ¨Avances en técnicas Biométricas y sus aplicaciones en seguridad¨(2017).

[20] Maya Vargas Adriana, "Sistema biométrico de huella dactilar en control de acceso entrada y salida" (2013).

[21] CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. Diario Oficial No. 48.587 de 18 de octubre de 2012.Ley estatutaria 1581 de 2012. Recuperado de: http://www.secretariasenado.gov.co/sena.

[22] MINTIC Ley 1273 de 2009 Recuperado de: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[23] Etchart Graciela, Alvez Carlos, Benedetto Marcelo, Fernández Miguel "Aplicación de sistemas biométricos en la administración pública loca para protección de la información" (2013).

[24] González Cervantes Julio César, "Vulnerabilidades de seguridad en las empresas" (2013).

[25] Cabarique Álzate Wilmar A., Salazar Romaña César Augusto, Quintero Barco Yeiler A., ¨Factores y causas de la fuga de información sensible en el sector empresarial¨ (2015).

[26] López Arguello Mariela E., ¨La cultura en seguridad de la información y su relación con la confidencialidad en UNIFINSA de la ciudad de Ambato¨ (2013).