engineering proceedings

Abstract

Hardware Passwords Manager Based on Biometric Authentication [†]

Camelia Avram [1,*], Jose Machado [2] and Adina Aştilean [1]

[1] Automation Department, Technical University of Cluj-Napoca, Memorandumului St., 400112 Cluj-Napoca, Romania; adina.astilean@aut.utcluj.ro

[2] MEtRICs Research Center, Campus of Azurém, University of Minho, 4800-058 Guimarães, Portugal; jmachado@dem.uminho.pt

[*] Correspondence: camelia.avram@aut.utcluj.ro

[†] Presented at the 8th International Symposium on Sensor Science, 17–28 May 2021; Available online: https://i3s2021dresden.sciforum.net/.

Abstract: This paper presents a portable passwords manager which has a two-stage biometric-based access procedure. Data security using biometric methods was chosen as a variant of reduced complexity but was very effective in preventing cyber theft. The implementation of biometrics for the purpose of identification in high-security systems has become essential with the evolution of technology and the spike in identity theft. Unlike passwords or IDs, a biometric feature is an identifier that cannot be lost, stolen, or replicated, which provides biometric authentication systems with an increased level of security. During the first accessing step, the 3DPassManager portable device measures the heartbeat and uses fingerprint and iris features to realize a unique biometric-based authentication. While the specific characteristics of fingerprint and iris features are integrated to ensure that the person using the device is the rightful owner, the pulse is utilized to verify if previously acquired static images are not used. During the second accessing step, a password is generated based on fingerprint details, valid only for a small-time interval. The fingerprint is stored in a secret key with a 1024-bit length. Once access is allowed, the passwords are made available through an extension installed on the web browser. The device is the size of a cigarette pack and communicates with the PC by scanning a QR code. It is safe and was previously tested for dictionary and brute force attacks.

Keywords: biometrics; authentication; sensors; portable; security

Supplementary Materials: The following are available online at https://www.mdpi.com/article/10.3390/I3S2021Dresden-10085/s1.

check for updates

Citation: Avram, C.; Machado, J.; Aştilean, A. Hardware Passwords Manager Based on Biometric Authentication. *Eng. Proc.* **2021**, *6*, 31. https://doi.org/10.3390/I3S2021Dresden-10085

Academic Editors: Gianaurelio Cuniberti and Larysa Baraban

Published: 17 May 2021