Hardware passwords manager based on biometric authentication

Authors: Camelia Avram, Jose Machado, Adina Aştilean

Abstract:

The paper presents a portable passwords manager having a two stages biometric based access procedure. Data security using biometric methods was chosen as a variant of reduced complexity, but very effective in preventing cyber theft. The implementation of biometrics for the purpose of identification in high security systems has become a must with the evolution of technology and the spike in identity theft. Unlike, passwords or IDs, a biometric feature is an identifier that can not be lost, stolen or replicated, fact that offers biometric authentication systems an increased level of security.

During the first accessing step, the 3DPassManager portable device measures heartbeat and uses fingerprint and iris features to realize a unique biometric based authentication. While the specific characteristics of fingerprint and iris are integrated to ensure that the person using the device is the rightful owner, the pulse is utilized to verify if possible previously acquired static images are not used. During the second accessing step, a password is generated based on fingerprint details, being valid only for a small time interval. The fingerprint is stored in a 1024-bit long key. Once the access is allowed, the passwords will be available trough an extention installed on the web browser. The device has the size of a cigarette pack and communicates with the PC by scanning a QR code. It is safe and was tested for dictionary and brute force attacks.

Key words:

Biometrics; Authentication; Sensors; Portable; Security.