NLock Release Presentation

Location : Neurotechnology Lab (Private) Limited - [Online]
Topic : NLock Presentation
Presenter : Rukshan (intern)
Date : 2016-03-29
Product version : v1.2 Beta

Introduction

Simple file locker

NLock is capable of locking your computer files and uses face biometric modality.

Users

Personal information hiding

Problems

- Distortion.
- No two captured templates of same person is same.
- Keeping templates discriminative power.
- Evolving with the Neurotechnology SDK

Related Approaches

- Biometric Encryption [3-8]
  - Key Binding
  - Key Generation
    - Does not save the template along with the data but some helper data.

- Cancelable biometrics [9-10]
  - "Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data."

Architecture

High Level Architecture
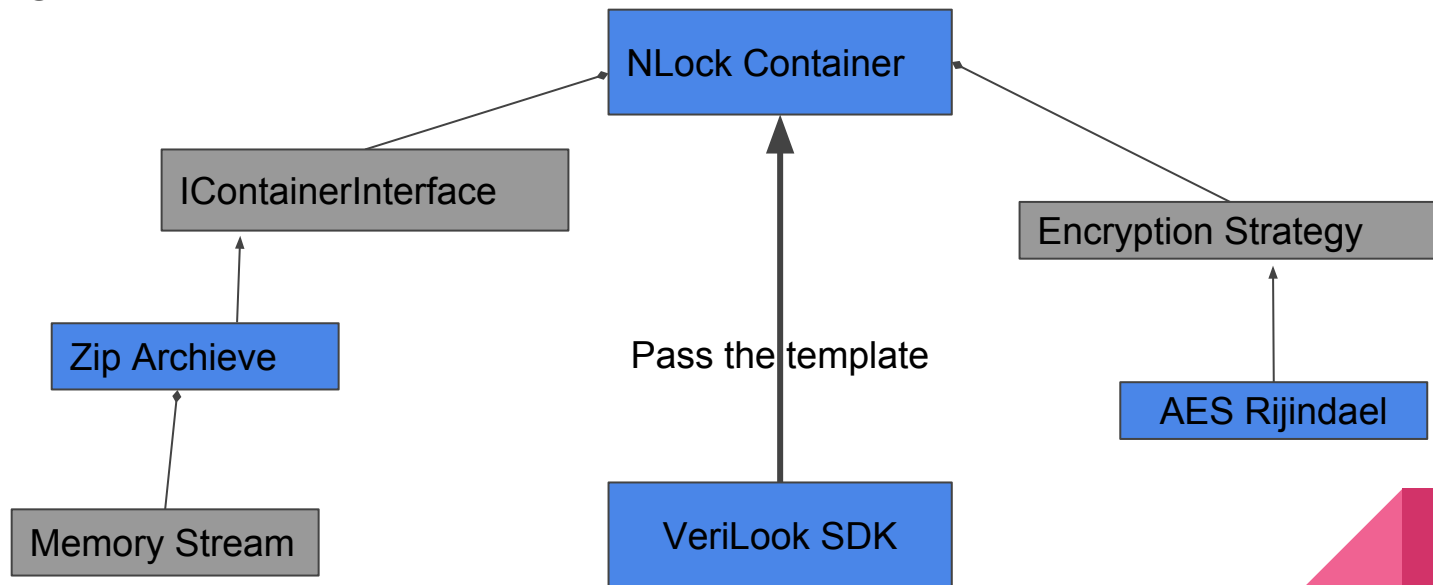
Concept

Locking

$$\text{Part1} = E_{(template)}(\text{content})$$

Concept

Locking

$$\textcolor{red}{\text{Part1}} = E_{(template)}(\textcolor{green}{\text{content}})$$

$$\textcolor{red}{\text{Part2}} = E_{(part1)}(\textcolor{green}{\text{template}})$$

Concept

Locking

$$Part1 = E_{(template)}(content)$$

$$Part2 = E_{(part1)}(template)$$

$$File = Part1 + Part2$$

Concept

Unlocking

Part1 and Part2

Concept

Unlocking

Part1 and Part2

$$\text{template} = D_{(Part1)}(Part2)$$

Concept

Unlocking

Part1 and Part2

template= $D_{(Part1)}(Part2)$

Verification

Concept

Unlocking

Part1 and Part2

template= $D_{(Part1)}(Part2)$

Verification

content = $D_{(template)}(Part1)$

Benefits

- No password based encryption weaknesses
    - People use passwords that they can easily remember.
    - Passcode can be used by another person.

Benefits

- No password based encryption weaknesses
  - People use passwords that they can easily remember.
  - Passcode can be used by another person.
- Integrated compression capabilities.

Benefits

- No password based encryption weaknesses
  - People use passwords that they can easily remember.
  - Passcode can be used by another person.
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.

Benefits

- No password based encryption weaknesses
  - People use passwords that they can easily remember.
  - Passcode can be used by another person.
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.
- Password based fallback option

Benefits

- No password based encryption weaknesses
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.
- Password based fallback option
- Windows integration

Examples

- Original NPointer.zip - 1.85 MB   NPointer.nlk - 1.89 MB
- xampp-win32-5.5.30-7-VC11-installer.exe - 105 MB
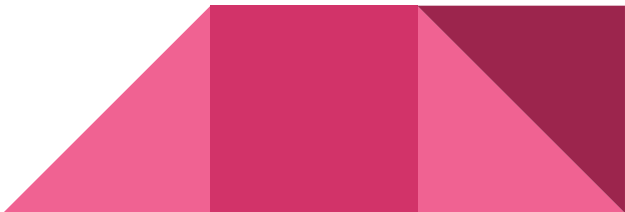 xampp-win32-5.5.30-7-VC11-installer.nlk   - 104 MB

NLock a start of a journey for biometric based file security and a different example for a new usage of Neurotechnology SDK.

References

[1] A. Cavoukian, A. Stoianov, and others, "Biometric encryption chapter from the encyclopedia of biometrics," Office of the Information and Privacy Commissioner, 2009. [Online]. Available: https://www.ipc.on.ca/images/Resources/bio-encrypt-chp.pdf..

[2] Biometric Encryption™ [Online]. Available: http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf.

[3] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in Advances in Cryptology–ASIACRYPT 2006, Springer, 2006, pp. 99–113.

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[5] "EU TURBINE" [Online]. Available: http://biometrics.org/bc2010/presentations/International/busch-Template-Protection-Projects-in-Europe.pdf.

[6] "Fuzzy extractor," Wikipedia, the free encyclopedia. 06-Oct-2015.

[7] "Reed–Solomon error correction," Wikipedia, the free encyclopedia. 04-Apr-2016.

[8] F. Hernández Álvarez, L. Hernández Encinas, and C. Sánchez Ávila, "Biometric fuzzy extractor scheme for iris templates," 2009.

[9] S. V. Gaddam and M. Lal, "Efficient Cancelable Biometric Key Generation Scheme for Cryptography.," IJ Network Security, vol. 11, no. 2, pp. 61–69, 2010.

[10] Y. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for face template protection," presented at the SPIE Defense and Security Symposium, 2008, pp. 694408–694408.

[11] J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection," Database, vol. 1, no. 3, p. 4, 2007.

Thank you..