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

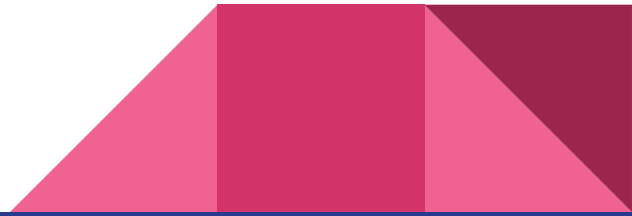
NLock is capable of locking your computer files and uses face biometric modality.

Users

Personal information hiding

Problems

- Distortion.
- No two captured templates of same person is same.
- Keeping templates discriminative power.



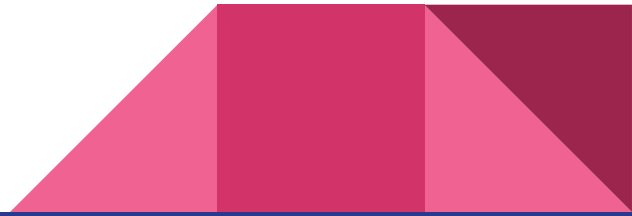
Related Approaches

- 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, 14]

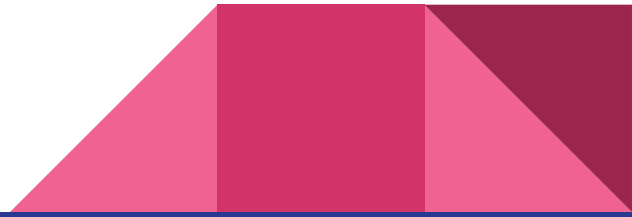
  “Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data.”



Concept

Locking

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

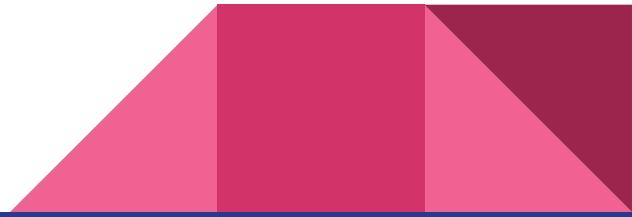


Concept

Locking

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

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



Concept

Locking

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

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

$$File = Part1 + Part2$$

Concept

Unlocking

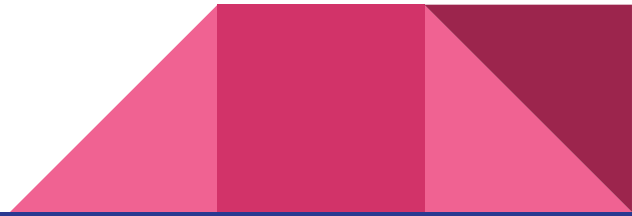
Part1 and Part2

Concept

Unlocking

Part1 and Part2

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



Concept

Unlocking

Part1 and Part2

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

Verification

Concept

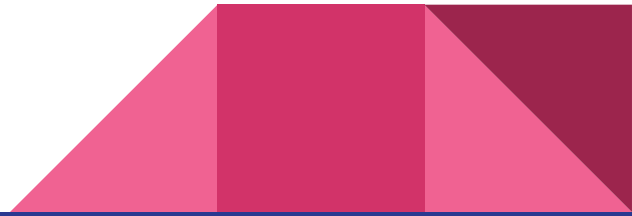
Unlocking

Part1 and Part2

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

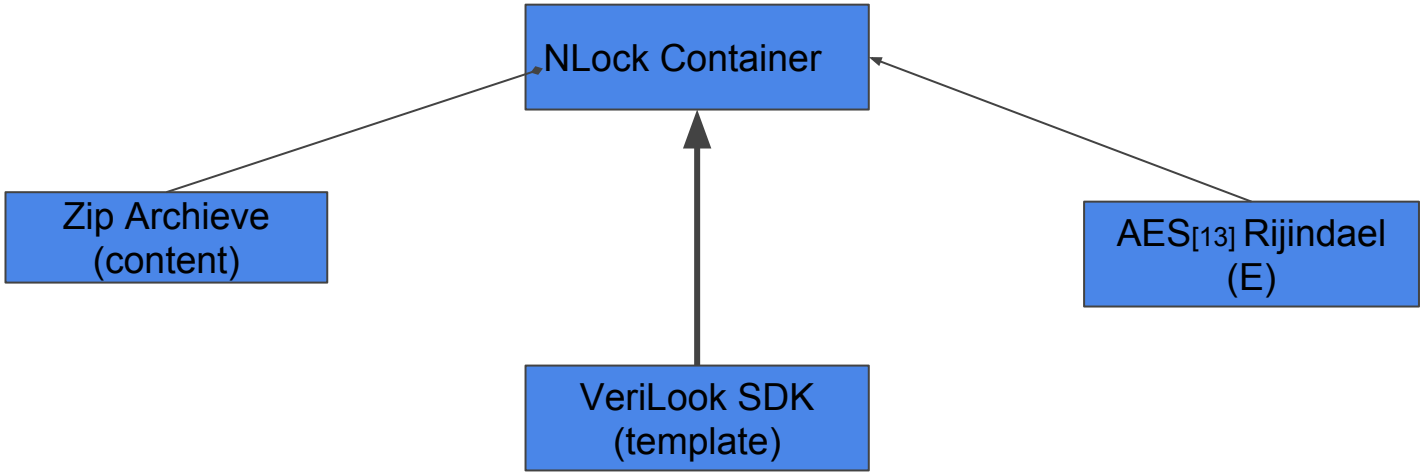
Verification

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



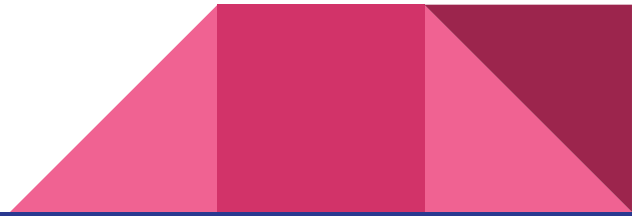
Architecture

High Level Architecture



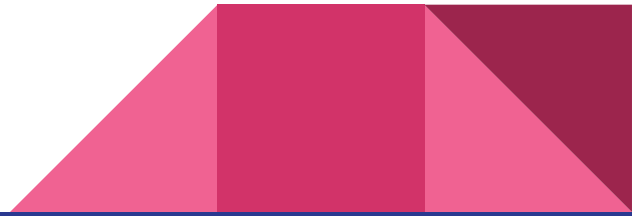
Benefits

- No password based encryption weaknesses [12]



Benefits

- No password based encryption weaknesses [12]
- Integrated compression capabilities.



Benefits

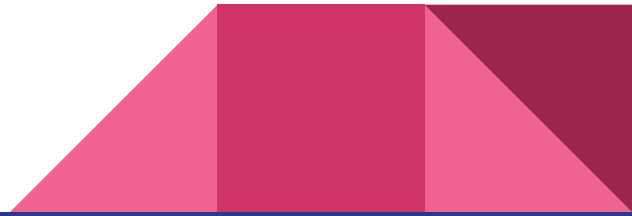
- No password based encryption weaknesses [12]
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.

Benefits

- No password based encryption weaknesses [12]
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.
- Password based fallback option

Benefits

- No password based encryption weaknesses [12]
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.
- Password based fallback option
- Windows integration

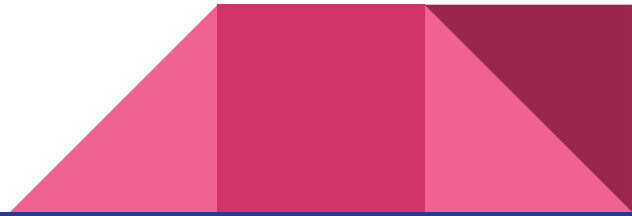


Benefits

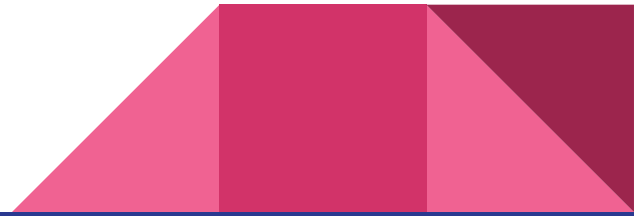
- No password based encryption weaknesses [12]
- Integrated compression capabilities.
- NLock shows how easy is to integrate Neurotechnology VeriLook SDK.
- Password based fallback option
- Windows integration
- Evolving with the Neurotechnology SDK.

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: http://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,. https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction

[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.

[12] D. V. Klein, “Foiling the cracker: A survey of, and improvements to, password security,” presented at the Proceedings of the 2nd USENIX Security Workshop, 1990, pp. 5–14.

[13] “Advanced Encryption Standard.” Wikipedia, the Free Encyclopedia, March 5, 2016. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[14] Ratha, Nalini K, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. “Generating Cancelable Fingerprint Templates.” Pattern Analysis and Machine Intelligence, IEEE Transactions on 29, no. 4 (2007): 561–72.

Thank you..

Attacks [1]

False Acceptance attack.
Reversing the hash
Hill Climbing attack
Nearest Impostors attack
Using statistics of ECC output