Jayme Woogerd
Comp 116 - Computer Security
October 29, 2014
Final Project Outline

Biocryptography: The Future of User Authentication?

I. Introduction

II. To the community

  A. Why I chose this topic
    1. Frustration with current state of user authentication systems
    2. Curiosity: are biometric systems as seen in popular culture (e.g. *Minority Report*) feasible? Creepy? Legal? "Better" than current traditional authentication systems?
  B. Why is this important?
    1. We already have a problem with password management (or lack thereof)
    2. The problem with password breaches is only going to get worse

III. Traditional methods in cryptography and their shortcomings

  A. Brief overview of cryptography
    1. General idea and definitions
    2. Private-key encryption and AES
    3. Public-key encryption
  B. Shortcomings
    1. Knowledge such as passwords and PINs can be easily forgotten (some stats about the average number of passwords people have to manage?)
    2. Passwords and PINs can be guessed using social engineering or dictionary/wordlist attacks (stats about breaches, etc?)
    3. Tokens like key or cards can be stolen or misplaced

IV. Traditional areas of biometrics and their shortcomings

  A. Brief overview of biometrics and biometric systems
    1. General idea and definitions
    2. Fingerprint systems
  B. Shortcomings
    1. Accuracy, security, and privacy challenges
    2. Biometric system attacks

V. Biocryptography methods and applications

  A. General overview and template protection
  B. Fingerprint Fuzzy-Vault Algorithm
  C. Others?

VI. Conclusion

Implementation: I plan to use a cheap fingerprint scanner or fingerprint images to implement a proof-of-concept biometric system using the Fuzzy-Vault algorithm to encrypt fingerprint data.

References

[1] *Details of the Data Encryption Standard*. http://www.quadibloc.com/crypto/co040201.htm.

[2] Ravi Das. *An Introduction to Biocryptography*, 2013 (accessed October 25, 2014). http://www.nationalhomelandsecurityknowledgebase.com/cln/news/2013/11221.aspx.

[3] Ravi Das. *Biometric Technology: Authentication, Biocryptography, and Cloud-Based Architecture*. CRC Press, 2014 (to be published November 10, 2014).

[4] Kai Xi and Jiankun Hu. Bio-cryptography. In *Handbook of Information and Communication Security*, pages 129–157, 2010.

(I plan to have many more sources; this is just a preliminary list.)