Biocryptography

The Future of User Authentication?

Jayme Woogerd

December 9, 2014

Abstract

In traditional cryptography, authentication relies on some sort of shared knowledge, usually a secret password or token. In today's wired world, these types of password authentication systems are pervasive – however, they face several fundamental problems, chief of which that they cannot distinguish between genuine users and attackers using stolen credentials. Biometric systems solve these problems by using physical uniquely identify genuine users. However, these systems come with their unique set of vulnerabilities.

At the intersection of biometrics and traditional cryptography lies biocryptography, which fuses the strengths of both types of authentication systems. This project explores the state-of-the-art strategies in biocryptography to provide systems that are both accurate and robust to attacks.

1 Introduction

In traditional cryptography, authentication relies on some sort of shared knowledge, usually a secret password or token. In today's wired world, these types of password authentication systems are pervasive – however, they face several fundamental problems, chief of which that they cannot distinguish between genuine users and attackers using stolen credentials. Additionally, users are forced to manage multiple accounts with multiple passwords.

Biometric systems solve these problems by using characteristics like fingerprints, irises, even ear shape to uniquely identify genuine users. However, these systems come with their unique set of vulnerabilities: what happens if a user's biometric data is compromised? A password can be easily reset...but a fingerprint certainly cannot. At the intersection of biometrics and traditional cryptography lies biocryptography, which fuses the strengths of both types of authentication systems. This paper explores the state-of-the-art strategies in biocryptography to provide systems that accurately authenticate genuine users and are robust to traditional biometric attacks.

2 To the Community

A. Why I chose this topic Frustration with current state of user authentication systems 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

3 Traditional Cryptography

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

4 Traditional Biometrics

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

5 Biocryptographic Methods and Applications

A. General overview and template protection

B. Fingerprint Fuzzy-Vault Algorithm

C. Others?

6 Conclusion

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.