Biocryptography

The Future of User Authentication?

Jayme Woogerd

December 10, 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 characteristics to 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

According to the results of an online registration and password study conducted by Janrain in 2012, 58 percent of adults have five or more unique passwords associated with their online logins and 30 percent of people have more than 10 unique passwords they need to remember. Additionally, almost 2 in 5 (37%) have to ask for assistance on their user name or password for at least one website per month [Janrain, 2012].

The current models for user authentication have created a ridiculous situation: on the one hand, experts implore us that a password should be long, random (and therefore not memorable) and unique so as to be resistant to cracking, but on the other hand, we have to create, keep track of, and periodically change credentials for *every single* service we sign up for. Anecdotally, for most people convenience trumps security and they end up using (and reusing) weak passwords over and over again.

The problem with password breaches is only going to get worse

Thus, the original motivation for this project was my own frustration with the current state of user authentication systems. It's deeply unsatisfying that so much of the onus is on the user to manage and secure her own credentials. Therefore, this project explores an alternative to a password-based authentication system: biometric systems and the biocrytographic methods used to secure them. I wanted to know if biometric systems as seen in popular culture (e.g. *Minority Report*) are even feasible and if so, in what ways are they better than current traditional authentication systems.

3 Traditional Cryptography and Authentication

The basic idea in cryptography is to allow two entities to send and receive messages to each other securely and confidentially in the presence of a third-party, or adversary. This is done through the process of data *encryption*, that is, transforming the message into an unreadable form to anyone who does not know how to decrypt it. In general, there are four main goals of modern cryptography: 1) confidentiality, 2) data integrity, 3) non-repudiation, and 4) authentication [Xi and Hu, 2010].

3.1 Authentication Systems

3.2 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 Biometrics

Rather than relying on a shared secret or key, in biometric systems, authentication relies on the physiological or behavior features of a person. Genuine users are recognized using characteristics like fingerprints, irises, or even ear shape. Biometric systems can be more reliable than traditional password-based systems because biometric features cannot be lost or forgotten and they are difficult to copy or forge and to share or distribute [Fengling Han, 2007].

4.1 Fingerprint Systems

Fingerprint systems are the oldest and most commonly used systems in biometrics.

4.2 Shortcomings

1. Accuracy, security, and privacy challenges

2. Biometric system attacks

5 Biocryptographic Methods and Applications

Because of the characteristics of fingerprint images, traditional methods like DES and RSA cannot be used for encryption. There characteristics include bulk data capacity and high correlation among pixels.

5.1 General overview and template protection

5.2 Fingerprint Fuzzy-Vault Algorithm

6 Conclusion

References

[DES, 2014] (2014). *Details of the Data Encryption Standard*. `http://www.quadibloc.com/crypto/co040201.htm`.

[Das, 2013] Das, R. (2013). *An Introduction to Biocryptography*. `http://www.nationalhomelandsecurityknowledgebase.com/cln/news/2013/11221.aspx`.

[Das, 2014] Das, R. (2014). *Biometric Technology: Authentication, Biocryptography, and Cloud-Based Architecture*. CRC Press.

[Fengling Han, 2007] Fengling Han, Jiankun Hu, X. Y. Y. W. (2007). Fingerprint images encryption via multi-scroll chaotic attractors. *Applied Mathematics and Computation*.

[Janrain, 2012] Janrain (2012). Online americans fatigued by password overload janrain study finds. `http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/`.

[Xi and Hu, 2010] Xi, K. and Hu, J. (2010). Bio-cryptography. In *Handbook of Information and Communication Security*, pages 129–157.