Jayme Woogerd
Comp 116 - Computer Security
October 14, 2014
Final Project Abstract

Biocryptography: The Future of User Authentication?

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 project will explore the state-of-the-art strategies in biocryptography to provide systems that accurately authenticate genuine users and are less vulnerable to traditional biometric attacks.