MIS6130 - INFORMATION SYSTEMS SECURITY, CONTROL AND AUDIT

THE ROLE OF BIOMETRICS IN ENHANCING SYSTEMS SECURITY, SYSTEMS CONTROLS AND SYSTEM AUDITING

Arthur Buliva
645381
abuliva@usiu.ac.ke

March 17, 2016

Contents

Chapter 1

Introduction

Biometrics is the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity. This paper will discuss the role biometrics would have in enhancing an ICT systems security. We will also analyze the role of Biometrics in System Auditing.

1.1 Biometrics at Large

Biometrics are generally classified into two broad categories:

1.1.1 Physiological Biometrics

Physiological characteristics are related to the shape of the body. This is also about the features of a person that rarely, if ever, changes. Examples of physiological characteristics include

- Fingerprints
- Retina recognition

- Face recognition
- DNA

1.1.2 Behavioural Biometrics

Behavioural Biometrics are all about the pattern of behavior of a person. These include:

- Walking style
- Accent and voice intonation patterns
- Gait
- Typing rhythm, etc

Chapter 2

Why the Fuss?

Biometric technology is rapidly gaining popularity in Kenya. The implied safety of plain passwords are being challenged by the forgeries of such password tokens, forcing many IT stakeholders to look for something difficult to forge.

The most popular use of PIN systems in Kenya is through ATM systems and SIM card PIN numbers. Integrating biometric systems with ATM transactions would indeed go a long way in reducing the risk of fraudulent withdrawals.

The downside of using biometrics is the potential of invasion of privacy that may occur when these characteristics are widely adopted. While debatable, and certainly not to be casually dismissed, the benefit of using biometrics in identity management far outweighs the risk of non-use.

Regardless of the identified challenges, biometric technologies seem to be gaining popularity in Kenya. The technologies tend to provide an alternative or complementary addition to the authentication problem of password and token-based systems - knowledge of a password, or the possession of an authentication token does not distinguish a person uniquely.

Chapter 3

Implementation of Biometric Systems in Kenya

Whenever biometric systems are being designed and deployed, there are some fundamental questions that need to be addressed:

1. Which is the most suitable form of technology that has all the required features?
2. How and where will the feature templates or images be stored?
3. Will there be exclusive biometrics or will there be complementary password or access card authentication features?
4. If there are complementary cards, will the images be stored in a central server or on the cards?
5. How will all the modules communicate with each other?
6. What are the guidelines, policies and procedures that are in place to ensure privacy and security of the system?

Of all these concerns, privacy is perhaps the biggest concern in the Kenyan context. People are usually skeptical of technologies that make use of their physical data, because the superstiotions that abound are such that they are all about *kunyonya damu* (translates directly to "sucking blood", though the meaning kind of loses its oomph in translation).

Privacy, which is a fundamental human right, is part of numerous international human rights instruments. It also supports and reinforces other rights, such as freedom of expression, information and association. Because biometric technologies employ really deep human traits about ourselves, it means that there is an imperative need to ensure that user privacy is maintained.

Indeed, Kenya has enacted several laws that aim to ensure privacy is maintained. Article 31 of the Constitution of Kenya protects the rights to privacy:

```
Every person has the right to privacy, which includes the right not to
have -
(a) their person, home or property searched;
(b) their possessions seized;
(c) information relating to their family or private affairs unnecessarily
required or revealed; or
(d) the privacy of their communications infringed.
```

There is a real and huge risk of invasion of privacy. A masquerader can very easily impersonate another person by planting their fingerprints on a crime scene, for example. Criminals can easily track their victims in the case of behavioural patterns, by predetermining their locations and striking when the victims are at the expected position.

The data collected also needs to be further cleaned because the material used to create fingerprint readers may affect the quality of the prints. Rogue users can also place a film on top of the reasers in order to skim prints off the devices and impersonate other people.

Being a relatively new technology in the Kenyan context, biometric technology is yet to be widely adopted in various situations in the country. Just as with any new technology, Kenya is generally considered to be an early adopter. Biometric technology has shown in the western world that it can really increase convenience as well as security of many systems.

Chapter 4

Enhancing System Security, Controls & Auditing

It is very difficult to forge a retina pattern. Unless you got the actual eyeball itself. And even so, any given human has a different retina scan on the right eye as compared to the left eye. This is just an example that goes to show how successful a proper deployment of a biometric system is when it comes to ensuring security and authorised access. Such is an example where biometrics really shine when it comes to security.

One major hurdle when it comes to this is that if a system is so configured that only one person can unlock it, it makes it difficult to do maintenance if the holder of the authentication is unavailable because of any given reason.

With such systems though, it is very easy to create an audit trail of events. Anything that happens within the system – from logging in to updating a record – has a possibility of being tracked with non-repudiation.

Bibliography

[1] Christos K. Dimitriadis, *BiometricsRisks and Controls* 2004

[2] Pauline Wamere, *Biometric Personal and Informational Privacy Concerns: A Kenyan context.* United States International University - Africa 2015

[3] Christos K. Dimitriadis, *BiometricsRisks and Controls* 2004

[4] Robert Gellman *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries* 2013

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK