BIOMETRIC SYSTEMS

Name

Presented to

Course

University, City

Date

Introduction

Biometrics technology is more valuable and effective than traditional technology system. Opposite to what most think, biometric technology has been there since 1879 when Alphonse Bertillon advocated for the use of anthropometric information for police investigations. This is the best method of investigating and resolving crimes police of today use. In addition, fingerprints were used in 1928 for women clerical workers of Los Angeles police and nowadays, biometric authentication systems have hundreds of applications in real life situations (Jain, A, Ross, and Pankanti, 2006).

The debate about which between traditional and biometrics technology is better is now over as the applications of biometric methods has become a basic institutional and policing need. Biometric technology finds its use in e-commerce, border patrol, criminal identification etc. The main reasons why everybody wants to use biometric technology are security betterment and authentication process for a user. Tradition technology systems use mainly password and other forms of authentication or verification and this is not enough to handle the ever evolving world of business and security. Traditional systems are important, but not as effective as biometric systems. Since the traditional methods are already known, it is more in place to adequately discuss the operational mechanism and performance metrics of a biometric system.

Biometric systems have obvious merits, but it is imperative to admit that, with everything comes a problem; biometrics technology works on a measurable percent similarity (100% match is never attained) suggesting there accuracy issues here. Authentication of voice or appearance cannot be as accurate as password verification. Biometric technology also has critical

vulnerabilities and operability problems. The invention of this technology came with more questions than answers. Can systems really rely on biometric technology?

The meaning of biometrics is basically the measurement of life and is derived from two Greek words “bios” and “metron”. In an IT security perspective; however, biometrics is defined as “authentication techniques that rely on measurable physical characteristics that can be automatically checked”.

The use of biometric technology has been tested and proved to be working more effectively. Evidence of scientific proving also shows that biometric technology provides more reliable and consistent information. Two look-alikes can be told apart by this method as it is able to recognize biometric dissimilarity (El-Abed & Charrier, 2012).

A biometric modality is any biometric information that can be used to distinguish persons and they include face, fingerprint, gait, keystroke dynamics, DNA, iris, voice, and hand geometry.

These modalities have something to fulfill. Biometric techniques are used for commercial purposes. The pie chart below shows percentage market share of each technology.

An automated method usually captures a biometric sample. Fr a sample to be captured, three things are necessary. (1) A biometric sensor - a mechanism for scanning and capturing a digital image of a living person characteristic; (2) A computer algorithm that compresses, processes and compares the image and (3) interface that has application systems to provide a similarity percentage.

The primary roles of a biometric system are to identity and verify information. Verification is different from identification, so companies and organizations procure biometric

systems in accordance with their needs. Identification and verification are performed by separate biometric systems, meaning a single system cannot perform both (Shutt, 2003).

Shutt (2003) says argues that for the biometric system to be considered a success, it must be able to distinguish false data. A voice recognition biometric system should tell if the voice command comes from the mouth of a living person, a robot, or an audio recording. It must also tell apart two voices from even identical twins. Although the system plays by percentage accuracy, the system must be able to at least register a 75%-85% match; otherwise there is no use of it.

The biometric method also recognizes physiological and behavioral characteristics of a person. The system should therefore, be able to use these characteristics to improve performance. Since almost all biometric techniques recognize the phycology and behavior of living persons, the technology is already booming in the market ("Opinion 3/2012 on Developments in Biometric Technologies")

The performance of a biometric system can be measured using transaction time, false accepts and false rejects. The biometric system is also flexible to handle high or low potential false accepts. The system is oversensitive to very large numbers of false accepts or false rejects, but very small numbers of false rejects or small numbers of false accepts might go unnoticed.

False acceptance rate (FAR) and false rejection rate (FRR) are the main sources of errors regarding biometric systems.

This is where a non-authenticated person is accepted by the system as authenticated. This happens when the biometric data of the imposter looks similar to the legitimate user's. As a

security protocol, the FAR must be very small to raise suspicion False Accept Rates in present biometric systems is 0.0001%-0.1%.

False rejection happens when a legitimate user is blocked access by the biometric system. This occurs when the system fails to find the user's current biometric data similar enough to the master template located in the database. Users previously accepted will get tired of the system and refuse to use it if the FRR is high (Pradhan, 2015).

S stated earlier, biometric systems have limitations especially with matters to do with accuracy. The evaluation process is going to cover three main areas and these are (1) data quality, (2) usability and (3) security.

Data quality is the major factor affecting the performance of biometric technology systems. To understand the concept of quality better, character, fidelity, and utility have been discussed.

Here character is the quality of the individual's physical features; fidelity is the level of similarity between the biometric source and its sample; while utility is the effect of the biometric sample on the general performance of a biometric system.

The international standards of biometric systems assert that the quality of a biometric sample must be corresponding to its recognition performance. Samples that have bad quality have a poor recognition performance.

ISO 13407; 1999 (1999) define usability as, *"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use".* Effectiveness according to the same source implies that the user is

capable of completing the wanted task with a small effort. Efficiency means that the user should be capable of achieving the work easily and within the required time. Satisfaction is a measure of user's acceptance and the sense of fulfillment concerning the biometric system.

The security threshold is also affecting the performance of a biometric system. If the security threshold is set too low, the chances of the system to reject authorized users increases. If the security threshold is set to a high rate, the system becomes so lenient that it accepts non-authorized users. The set of the security threshold hugely depends on the needs of the organization. For convenience-oriented organizations, the biometric system must be set to a low acceptance rate and if the priority of the organization is security, then the commercial biometric system must have a low false rejection rate. This is how the biometric machines work (Shutt, 2003).

In conclusion, the modern business, institutional and policing world desperately needs biometric systems for identification and verification. Traditional systems can also be used as supplement to biometrics, but the latter is the backbone of information systems. Biometric systems have their own shortcoming, but they are worth investment.

Looking back half a century ago when very complex and ineffective traditional methods, it is clear that identification and verification procedures were time and effort consuming. With the current implementation of biometric systems even in election processes, traditional methods are gradually finding less significance by the day and it is only a matter of time before the latter disappears in totality.

The biggest drawback of biometric systems is the potential risk of identity theft. People would stop at nothing to steal biometric information and use it for their own selfish purposes including theft and escape, but these reasons are not sufficient to overrule the use of biometrics.

The concept of biometrics technology is a little bit complicated, but with time everyone will know how to use it. Remember when mobile phones and computers came in the market, they were dubbed as complex devices but presently even a 3 year old can send use a phone and a computer.

Similarly, neither the use of password is safe. Hackers will always get users and steal their password, so ownership breach concerns do not hold enough water to say that one system is better than the other; although more generally, biometrics techniques are more effective and their performance is of greater value that traditional systems.

RFERENCES LIST

Down, PM and Sands, JR. 2004. Biometrics: An Overview of the Technology, Challenges and Control Considerations. [Online]. Available at: <http://www.isaca.org/Journal/archives/2004/Volume-4/Documents/jpdf044-Biometrics-AnOverview.pdf> [Accessed 13 Aug 2015]

Polemi, D. 1997. BIOMETRIC TECHNIQUES: REVIEW AND EVALUATION OF BIOMETRIC TECHNIQUES FOR IDENTIFICATION AND AUTHENTICATION, INCLUDING AN APPRAISAL OF THE AREAS WHERE THEY ARE MOST APPLICABLE [Online] Available at: <.https://danishbiometrics.files.wordpress.com/2009/08/biomet.pdf http://www.planetbiometrics.com/creo_files/upload/article-files/btamvol1update.pdf > [Accessed 14 Aug 2015].

Shutt, J. 2003. A Comparative Study of Biometric Systems. [Online]. Available at: <https://vlebb.leeds.ac.uk/bbcswebdav/orgs/SCH_Computing/FYProj/reports/0203/Shutt.pdf>

[Accessed 13 Aug 2015].

El-Abed, M & Charrier, C. 2012. Evaluation of Biometric Systems. [Online]. Available at: <http://cdn.intechopen.com/pdfs-wm/41062.pdf> [Accessed 13 Aug 2015].

Pradhan, M. 2015. Next Generation Secure Computing: Biometric in Secure E-transaction. Nternational Journal of Advance Research in Computer Science and Management Studies. Vol. 3. No. 4. [Online]. Availabel at: <http://www.ijarcsms.com/docs/paper/volume3/issue4/V3I4-0131.pdf> [Accessed 13 Aug 2015]

http://research.ijcaonline.org/volume85/number9/pxc3893246.pdf

April 27th 2012. Developments in Biometric Technologies. *Article 29: Data Protection Working Party*. [Online] Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>

Jain, KA, Ross, A and Prabhakar, S. 2004. An Introduction to Biometric Recognition. Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1. [Online]. Available at:

<http://www.cedar.buffalo.edu/~govind/CSE717/papers/IntroductionToBiometricRecognition.pdf>

Jain, A, Ross, A, Pankanti, S. 2006. Biometrics: A Tool for Information Security. *IEEE Transactuions on Information Forensics and Security*, Vol. 1, No. 2. [Online] Available at: <http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainRossPankanti_BiometricsInfoSec_TIFS06.pdf> [Accessed 13 Aug 2015].

Chapter 13: Biometrics. [Online] Available at: <http://www.cl.cam.ac.uk/~rja14/Papers/SE-13.pdf> [Accessed 13 Aug 2015].