A CONCEPTUAL MODEL FOR THE INTRODUCTION OF BIOMETRICS INTO YOUR ORGANIZATION: A SIX-STEP PROCESS

Hossein Bidgoli, California State University-Bakersfield, hbidgoli@csub.edu

ABSTRACT

Security threats are on the rise and it has become a major challenge for systems managers, public and private officials to come up with new and more comprehensive security systems in order to keep the hackers and computer criminals at bay. Biometrics has attracted much attention after the September 11, 2001 attacks in the United Sates. Biometrics securities use a physiological element to enhance security measures. Biometrics offers certain characteristics not available in other security measures. The goal of this article is to present a systematic approach for the introduction of biometrics as a security measure into your organization. The article proposes a six-step guide that if followed should significantly increase the chances of success for using this fast growing technology. The steps are (1) understanding security threats and measures, (2) understanding access controls, (3) understanding biometrics measures, (4) understanding common applications of biometrics, (5) understanding sample case examples, (6) putting together a plan for implementation. The implementation plan is explored below.

THE IMPLEMENTATION

An organization's employees are an essential part of the success of any security initiatives including biometrics, so training and education on strengths and weaknesses of this platform and security awareness are important. In addition, making sure management supports the training program is important to help promote the adoption of this new technology throughout the organization. Biometrics security could be added as an extra layer of security on the existing security system or it could be employed for access control for those applications suitable for this

implementation. The following steps should be considered when introducing biometrics into your organization (Bidgoli, 2003, 2011):

1. Set up a security committee with representatives from all departments as well as upper management. The committee's responsibilities include the following:
   - Developing a clear, detailed biometrics acquisition and use plan
   - Providing biometrics awareness for key decision makers and users
2. Conduct risk analysis and assess the ROI of biometrics implementation and compare and contrast it against other security alternatives.
3. Define the organization's needs. A clear definition of needs will assist the organization to decide on a specific biometrics measure. For example for m-commerce applications voice recognition might be the preferred technique. However, with age, the voice of a person changes and a person with flu or sore throat has a different voice than normal and voice recognition may not provide accurate results. For database access fingerprint might work best. However, using fingerprints, the scanner must be kept clean. Dry, wet, or dirty hands may reduce the accuracy of the system. If a previous user has left a dirty spot on the scanner, or the finger isn't placed in the right position, the system may not work. The fingerprint of those people working in Chemical industries is often affected. Therefore these companies should not use the fingerprint measure for the authentication purpose.
4. Examine key characteristics of biometrics measures. The accuracy, cost, user acceptance, and reliability of all biometrics measures must be first assessed and then choose the measure that provides the best match for a particular application. Table 1 lists key characteristics of biometrics measures.

Table 1

Key Characteristics of Biometrics Measures

Biometrics Measures	Accuracy	Cost	User Acceptance	Reliability
Facial recognition	Medium-low	Medium	High	High
Fingerprints	High	Low	Medium	High
Hand Geometry	Medium-low	Low	High	High
Iris Analysis	High	High	Medium-low	Very high
Palmprints	High	Low	Medium	High
Retinal Scanning	High	High	Low	Very high
Signature Analysis	Low	Medium	High	High
Vein Analysis	High	Medium	Medium	High
Voice Recognition	Medium	Medium	High	High

5. Examine the providers of biometrics platforms and match their offerings against your needs, not all vendors are equal. Choose the provider whose offerings are the closest to your needs. Also other variables that set a good vendor apart from the rest such as user support, reputation, number of years in business, and number of customers should be considered.

CONCLUSION

With ever increasing threats toward data resources and national and homeland security biometrics could play a major role in order to keep hackers and criminal at bay. By a careful literature review, examination of several real life applications, and understanding major biometrics measures strengths and weaknesses, and their common applications this article

introduced a six-step guide for introducing biometrics into your organization. If these steps are carefully followed, they should increase the chances of success for the introduction and utilization of this fast growing technology.

REFERENCES

Anderson, H. (2010), "Case Study: The Motivation for Biometric", *HealthcareInfoSecurity.com*, available at: http://www.healthcareinfosecurity.com/articles.php?art_id=2686 (accessed 2 May 2011).

Aponovich, D. (2001), "Biometrics Eases City's Network Access Security Woes", *Datamation*, available at: http://itmanagement.earthweb.com/secu/article.php/863861/Case-Study-Biometrics-Eases-Citys-Network-Access-Security-Woes.htm (accessed 2 May 2011).

Bidgoli, H. (2003), "An Integrated Model for Improving Security Management in the E-commerce Environment, *Journal of International Technology and Information Management*, Volume 12, Number 2, pp.119-134.

Bidgoli, H. (2011), MIS2, Course Technology/Cengage Learning, Mason, OH.

Biometrics: The future of security (2004), *CBC News Online*, available at: *http://www.cbc.ca/news/background/airportsecurity/biometrics.html*, (accessed 2 May 2011).

Buenaventura, D. (2011), "Some Interesting Statistics on Security Breaches on the Internet", *Bright Hub, Inc*., available at: http://www.brighthub.com/internet/security-privacy/articles/112421.aspx (accessed 2 May 2011).

Mesenbrink, J. (2002), "Biometric Plays Big Role with Airport Security," *Security Magazine*, available at: *http://www.securitymagazine.com/articles/biometrics-plays-big-role-with-airport-security-1* (accessed 2 May 2011).