Communications of the IIMA

Volume 6 | Issue 2 Article 7

2006

Bioinetric and Systems Security: An Overview of End-To-End Security System

Emmanuel Opara
Prairie View A & M University

Mohammad Rob
University of Houston

Vance Etnyre
University of Houston

Biometric and Systems Security: An Overview of End-To-End Security System

Emmanuel Opara
Department of Management Information Systems,
College of Business, Prairie View A&M University, Prairie View, Texas 77446

Mohammad Rob
Department of Management Information Systems, School of Business
University of Houston-Clear Lake, Houston, Texas 77546

Vance Etnyre
Department of Management Information Systems, School of Business
University of Houston-Clear Lake, Houston, Texas 77546

ABSTRACT

As online security threats continue to spread, protecting valuable data becomes one of the security challenges businesses face in today's business-to-customer (B2C) and business-to-business (B2B) e-commerce. Biometrics technology shows increased promise in enterprise network security. It will play a vital role as system developers fortify the security apparatus of its organization. In this paper, we analyze biometrics technologies and describe techniques that can be utilized to decrease the probabilities of online attacks.

INTRODUCTION

Secured online access to enterprise resource is important for organizations that are striving to sustain their competitive advantage in today's business environment. As online security threats continue to spread, protecting valuable data becomes one of the security challenges businesses face. Enterprise customers and clients involved in business-to-customer (B2C) and business-to-business (B2B) e-commerce need to feel secured and confident that their transactions are secured from system hackers.

Security is necessary to maintain secrecy of important information (Ross, et al., 2005). For businesses to remain competitive, strategic business partners within the systems must share secrets and transport data during business transactions. The adequate methodology to prevent an intruder from entering the network system is to provide a security apparatus between the intruder and the corporate network. The question is how to authenticate users to servers as well as authenticate servers to users, so as to secure both client and server computers from potential attacks.

Biometrics technology provides a solution to this problem. It has been widely used in hospitals for controlling access to medical/patient files, and forensic analysis such as prison security control and criminal identification. Biometrics technology measures physiological and or behavioral characteristics that are used to verify the identity of an individual. Although the market for physical access control to an enterprise computing environment is currently dominated by token-based technology, the rapid progression of biometric technology will shift the enterprise security needs to biometric techniques (Kohler et al., 2004).

Integration of biometric systems into the general security protocol is critical to the successful deployment of biometric technologies. As data move between enterprise network and various systems, adequate care must be ensured to avoid systems vulnerabilities. These include identity, reply and hill-climbing attacks as various interfaces become standardized. Biometric technology will play a vital role as system developers fortify the security apparatus of its organization. The implementation of the biometric application programming interface (BioAPI, 2001) has made it possible for the integration of biometric systems into enterprise applications. The theory behind this consideration is for system security analyst to identify and prevent any potential security attacks that could be mitigated as a result of biometric usage. A comprehensive integration of the interface between biometric systems and enterprise security systems is paramount to system security.

In this paper, we analyze biometrics technologies and the potential attacks it face. We will evaluate measures that can be utilized to decrease the probabilities of such attacks.

LITERATURE REVIEW

Uludag et al. (2004) defined biometric technique as an automated methodology for the recognition of a person based on behavioral or physiological characteristics. These characteristics include features such as hand geometry, handwriting, face, fingerprints, vein, voice, retina, and iris. The authors concluded that biometric technologies are now the key to an extensive array of highly secured identification and personal verification solutions. Welzl (2004) states that the biometric system is a pattern recognition technology that makes personal identification of an individual by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user.

Jain et al. (2003) describe the significant differences between the physiological and behavioral biometrics. The physiological biometrics consists of measurements and data congregated from direct measurement of a part of the human body. Samples of these include but not limited to hand geometry, facial recognition, fingerprint, iris-scan etc. On the other hand, the behavioral characteristics originate from the actions of an individual, and it indirectly measures unique characteristics of the human body. Samples of these include but not limited to signature-scan, keystroke-scan, voice recognition, etc. Time can act as a metric for behavioral biometrics, because it measures behavior by considering the timeline of a given process (Shoniregun, 2003; Ratha et al., 2001; Putte and Keuning, 2000).

Jain and Uludag (2003), and Soutar (2002), among others noted that an ideal biometrics system should be universal, unique, permanent and collectable. It must be universal that every person possesses the characteristics and uniqueness; where no two persons share the characteristic and permanency; where the characteristic should neither be changed nor be alterable; and finally the characteristics must be collectable and be readily presentable to a sensor and is easily quantifiable (Uludag, et al., 2004). Some other studies found that characteristics that satisfy all the above mentioned requirements may not be practical or feasible for a useful biometric system (Linnartz and Tuylus, 2003).

Schneier (1999) and Timmers (2000) in their studies indicate that the integration of biometric technologies into applications was achieved using proprietary software developers' kits (SDK's). However more recent studies summarized that a standardized biometric application programming interface, BioAPI, version 1.1 of the specification released in 2001 was instituted to enhance the portability of unrelated biometric technology within applications (Soutar, 2002; Jain and Uludag, 2003; Adler, 2004).

Also, it was determined that developers and vendors of a practical biometric system should consider other issues such as performance, acceptability and circumvention (Ross et al., 2005). Performance in this sense means systems accuracy, speed, robustness, as well as its resource requirements and operational or environmental factors that affect its accuracy and speed. Acceptability means the extent people are willing to accept a given biometric sample identifier in their daily lives. Circumvention means how easy it is to fool the system through fraudulent methods (Uludag et al., 2005).

Biometrics based authentication applications that is critical to the growth of the global economy comprises of many features. These include but not limited to single sign-on, Web security, transaction security, application logon, data protections, workstations, remote access to resources, and etc (Maltoni, 2003).

BIOMETRICS TECHNOLOGY AT WORK

The goal for a biometric system configuration for positive verification ensures that the object is the same that is enrolled in the security system as a template. Enterprise biometric template designed from a given sample is bound to an identifier by which they are known to the security system (see figure 1). The process continues as the identifier creates a link between the verification of the user with the biometric system and the authorization of the rights and privileges within the security system. It is to be noted that as interfaces are developed, system security could be compromised as information flows between the biometric technology, desktop, laptop or any personal computer applications

As shown in Figure 1, the fusing together of identifier to system biometric template is achieved by implementing an encryption/decryption technology within a trusted biometric system. This process creates a User Record which can be moved or stored on a portable medium such as a credit card, smart card etc.

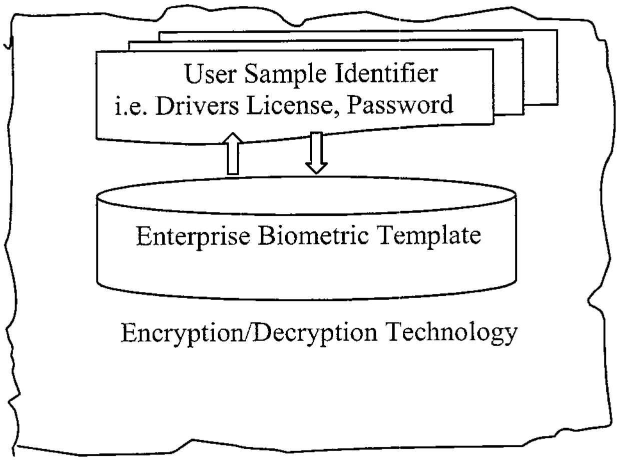
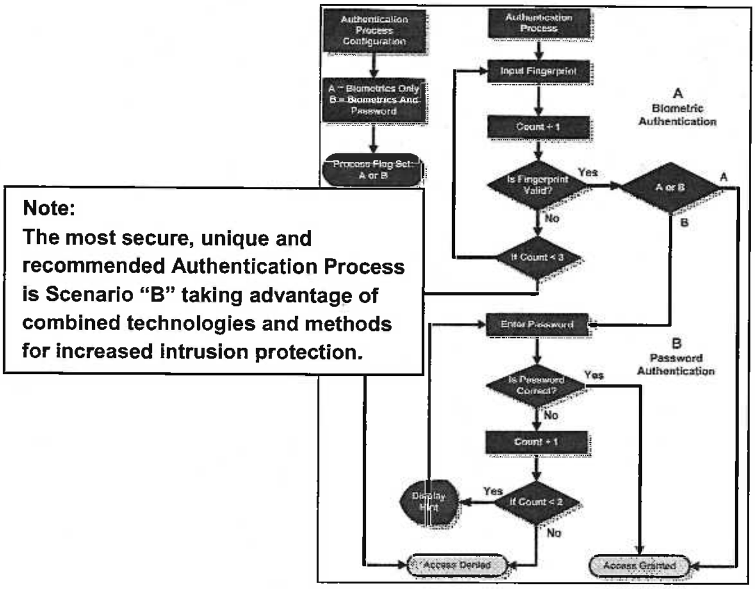

User Sample Identifier
i.e. Drivers License, Password
Enterprise Biometric Template
Encryption/Decryption Technology

Figure 1: Development of Biometric Template (Adapted from Adler, 2004)

One of the oldest among the biometric techniques is the fingerprint-based identification. This method had been very successful because everyone is known to have unique, immutable fingerprints. They are so unique because a fingerprint can be determined by a pattern of ridges and minutiae points. Figure 2 shows a flow chart that demonstrates the authentication process of a traditional password and biometric fingerprint identification. It begins with an input fingerprint sample. A threshold is set using a counter that is limited to three attempts for positive identification. If this process returns a negative identification, the user is prompted to contract the security administrator. If the user successfully passes the fingerprint test for positive identification, the system prompts for a password. Another threshold is set at this stage with two attempts for a positive password. When the user has been fully authenticated with the proper password, the user will access the system. It after the two hind for a positive identification and the response is negative; the user will be prompted to contact the system security personnel.

MANAGERIAL IMPLICATIONS

The major element to any secured environment is to understand exactly what elements are within such an environment. The equation "what you have + what you know {Pin} + what you are = identity confirmation" is a methodology system security analysts use to define identity. The challenge that lies ahead for system security gurus is how to validate an individual's identity to ensure accuracy since documents are easily counterfeited. Another problem is that passports are easily stolen and user passwords are also easy to forget. However, the study noted that no single piece of technology can be used to firmly secure all information on the superhighway. An integrated information security infrastructure that could safeguard enterprise systems will comprise of several technologies. These technologies include but not limited to firewalls that accept or deny traffic within networks, encryption systems that guarantees data integrity and confidentiality, passwords and biometrics that authenticate network users at the airports, boarders, buildings finances and at virtual private networks (VPNs).



Note:
The most secure, unique and recommended Authentication Process is Scenario "B" taking advantage of combined technologies and methods for increased intrusion protection.

Figure 2: Authentication process of a password and fingerprint identification

CONCLUSION

This study has shown that biometrics is the most accurate and secured representation of what an element is. Its technology can isolate false positive results, misrepresentation or creation of false identity during an identification process. We have discussed the usefulness of biometric technology in protecting enterprise network systems from unwanted online intruders. We have also identified the possible features and characteristics of an object that can be used in biometric technologies. Furthermore, an enterprise authentication process that uses a combination of traditional password and biometric fingerprint identification methodology is described.

FINDINGS AND FUTURE TRENDS OF BIOMETRIC SYSTEMS

Biometrics systems are sophisticated and advanced as compared to other identification solutions packages since the technology authenticates a person's identity base on a unique physical attribute rather than some form of identification formula. The exposure accorded biometric applications has enhanced awareness in the industry; however, the visibility could become problematic to the Industry in general.

Future biometric vendors struggling to meet compliance requirements will have to enter the market using the late-movers' strategy. However, those first mover-vendors that have met the increasingly rigid requirements for accuracy, universal enrollment and transparency, will experience an unprecedented surge for enterprise systems to employ biometric technology as solution for array of system customer-related applications.

REFERENCES

Adler, A. (2004), Images can be regenerated from quantized biometric match score data, *Proc. Canadian Conf. Electrical Computer Eng.*, pp. 469-472, (Niagara Falls, Canada).

BioAPI (2001), BioAPI Specification, American National Standards Institute, ANSI/INCITS 358, Version 1.1. Retrieved December 20, 2005 from http://www.bioapi.org/BIOAPI1.1.pdf

Jain, A. K. and Uludag, U. (2003), Hiding biometric data, IEEE *Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494-1498.

Kohler, E., Handley, M. and Floyd, S. (2004), RFC4340: Datagram Congestion Control Protocol (DCCP), Retrieved January 30, 2006from http://www.read.cs.ucla.edu/dccp/.

Linnartz J. P. and Tuylus, P. (2003), New shielding functions to enhance privacy and prevent misuse of biometric templates, *Proc. AVBPA 2003, Fourth International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 393-402, Guildford, UK.

Putte, T and Keuning, J. (2000), Biometrical fingerprint recognition: don't get your fingers burned, Retrieved November 20, 2005 from http://cryptome.quintessenz.org/mirror/fake-prints.htm.

Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001), An analysis of minuntiae matching strength, *Proc. AVBPA 2001, Third International Conference on Audio – and Video-Based Biometric Person Authentication*, pp. 223-228.

Ross, A., Shah, J. and Jain, A. K. (2005), Towards reconstructing fingerprints form minutiae points, *Proc. SPIE, Biometric Technology for Human Identification II*, Vol. 5779, pp. 68-80, (Orlando, FL).

Schneier, B. (1999), Inside Risk: The uses and abuses of biometrics, *Comm. ACM*, vol. 42, no. 8, p. 136.

Shoniregun, C.A., (2003), Are existing Internet security measures guaranteed to protect user identity in the financial services industry? *Int. J. Services Technology and Management,* vol. 4, no. 2, pp.194-216.

Soutar, C. (2002), Biometric System Performance and Security. Retrieved October 10, 2005 from http://www.bioscrypt.com/assets/bio_paper.pdf

Timmers, P. (2000) *Electronic Commerce (Strategies and Models for Business-to Business Trading),* John Wiley Publications, New York.

Uludag, U., Pankanti, S. and Jain, A. K. (2005), Fuzzy vault for fingerprints, *Proc. Audio- and Video-based Biometric Person Authentication (AVBPA),* (Rye Brook, NY), July.

Uludag, U., Pankanti, S., Prabhakar, S, and A.K. Jain (2004),Biometric cryptosystems: issues and challenges, *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960.

Welzl, M. (2004), TCP Corruption Notification options, *Internet-draft (*work in progress) draft-welzl-tcp-corruption-00.txt, June 2004. Retrieved February 12, 2006 from http://www.ietf.org or http://www.welzl.at/research/publications.