Chapter 3.5
Biometric Controls and Privacy

Sean Lancaster
Miami University, USA

David C. Yen
Miami University, USA

ABSTRACT

Biometrics is an application of technology to authenticate users' identities through the measurement of physiological or behavioral patterns. The verification system offers greater security to the use of passwords or smart cards. Biometric characteristics cannot be lost or forgotten. As biometric characteristics are concerned with the very makeup of who we are, there are also security, privacy, and ethical concerns in their adoption. Fingerprint, iris, voice, hand geometry, face, and signature are all considered biometric characteristics and used in the authentication process. Examples of everyday biometric applications include thumbprint locks on laptop computers, fingerprint scanners to enter a locked door on a house, and facial recognition scans for forensic use. While there are several examples of biometrics currently in use, it is still an emerging technology. The purpose of this chapter is to provide a descriptive discussion of the current and future state of biometrics.

INTRODUCTION

The world is growing increasingly digital as information systems and networks span the globe. As individuals, customers, employees, and employers, we can often connect to the Internet, and to our information systems, from anytime and anywhere. The freedom and flexibility that technology provides is truly astounding when compared to the limits placed on society just a few years ago.

Furthermore, data is recognized as a valuable resource. The information and knowledge that is created with this data is vital to business, trade, and the increased convenience of common day-to-day activities. We use this data to answer a variety of questions. Companies collect and aggregate data on their customers, products, and competitors. Individuals save confidential files on their hard and soft drives. How is this data secured? How

DOI: 10.4018/978-1-61350-323-2.ch3.5

are the physical and digital systems that store this data secured? How can we, as citizens of a digital society, protect ourselves from the theft of this private data? If you do not trust the information you are working with, you will not trust the decisions made with that data's analysis.

Biometrics is becoming more and more common as an answer to those questions. Biometric devices are a means of authenticating user identity or identifying someone from a list of possible matches. This chapter will cover why biometrics is needed, how they are used, important issues in their adoption, and future trends in their evolution. Learning Objectives:

- Learn the significance of privacy and the risk of identity theft
- Better understand the need for biometrics in modern society
- Comprehend the technical, economic, business, and ethical issues related to biometrics

THE NEED FOR BIOMETRICS

Imagine the most typical of e-commerce transactions, purchasing an item from an online Web site. You select the merchandise and begin to check out by filling in your personal information to complete the order. Now, also imagine someone standing over your shoulder watching and recording the data that you submit. Even worse, once you are finished, this person uses that data to impersonate you, accessing and using your credit.

Fraud and identity theft are common examples of cybercrime. The United States' Federal Trade Commission reported nearly 700,000 cases, with losses totaling nearly $700 million, of identity theft and online fraud during 2005 (Consumer Fraud, 2006). The same report from the FTC listed the most common methods consumer information was misused. A summary of that list can be found in Figure 1.

A key aspect of both fraud and identity theft is the ability of the cybercriminal to impersonate the victim while convincing others of the fraudulent identity. This is especially true for systems that require only passwords, user logins, or simple ID swipe cards. For each of these, cybercriminals are able to obtain the password, login, or card through techniques that range from human engineering to user carelessness to sophisticated software programs. Once the cybercriminal has obtained the password or ID card, there is little to stop them from impersonating the victim. The password and card provide access to the prey's physical and digital systems and assets. Examples

Figure 1.