SRMG HOT TOPIC: SECURITY TECHNOLOGY

INTRODUCTION: BIOMETRICS

Ever since the September 11 terrorist attacks, there has been a higher level of concern regarding safety and security measures and a need to improve them at U.S. borders, airports, and public areas. For this reason, both the government and private corporations are turning their attention to the field of biometrics.

The science of biometrics involves analyzing biological, physiological, and/or behavioral characteristics that are unique to a single individual and using them to recognize or verify the identity of that human being. Today, biometric technologies are typically used to analyze human characteristics for security purposes.

There are several different types of biometric technologies, i.e., iris (eye) scanning, retinal recognition, facial recognition, fingerprint recognition, hand geometry, voice recognition, infrared imaging, keyboard dynamics, and handwriting dynamics. A few new, innovative approaches are also being examined to determine their potential for use in biometric analysis, such as ear shape, Deoxyribonucleic Acid (DNA), keystroke (typing) rhythm, and body odor.

Some biometric technologies are more reliable than others, but they are all based on characteristics considered to be unique to a single individual. For example, it is common knowledge that no human being has the same fingerprint as another. Therefore, fingerprinting is a reliable technology. On the other hand, systems that utilize voice recognition or keyboard dynamics and patterns are less reliable since both voices and typing styles can be mimicked.

Because of the high costs associated with biometric security measures, they are still in the developmental stages. However, these types of security systems are currently in limited use at airports, banks, and other institutions. Now that security has become a much higher priority worldwide, corporations and governments alike will have no choice but to take the necessary steps to protect themselves, their customers, and/or their citizens.

PROTECT YOUR PERSONAL INFORMATION/IDENTITY THEFT PREVENTION

Banks have begun to make use of biometric technologies to protect their patrons against identity theft.

- Bank United was one of the first banks to use biometrics. For more information, go to http://www.bankrate.com/brm/news/bank/20020723a.asp.
- Orange County's Credit Union (OCCU) in Orange County, California requires a thumbprint and signature scan for all new accounts and also offers this security option to customers with existing accounts. This enables customers to open accounts without the assistance of any personnel.

However, due to the fact that Automated Teller Machines (ATMs) are so established worldwide, it would be very expensive to replace the standard four-digit Personal

Identification Number (PIN) with a biometric technology because of the need to develop and implement the necessary infrastructure to support it. An easier and cheaper solution would be to replace the current magnetic strip ATM debit cards with smart cards that can hold more information. These types of cards could be used in Microsoft Windows-based ATMs. For more information, go to http://atmmarketplace.com/news_story_22036.htm.

BIOMETRICS WHEN TRAVELING

Airports are using biometric technologies, such as iris (eye) scanning, to improve travel safety. Two of the first airports to begin scanning passengers' irises as part of an effort to streamline boarding and security processes were Charlotte Douglas International Airport (CLT) in North Carolina and Frankfurt Airport (FRA) in Germany in the year 2000. For more information, go to http://archives.cnn.com/2000/TECH/computing/07/19/iris.scan.idg/index.html.

BIOMETRICS AT WORK

Corporations are always faced with security issues such as employee identity theft, equipment theft, vandalism, and improper registering of hours worked. Additionally, they incur significant costs replacing lost or stolen building keys or access cards (badges) and correcting time and attendance issues. By implementing biometric systems, employers can develop an employee identification database to control access to particular locations and equipment based on specific clearance levels, prevent fraudulent time and attendance entries, and protect their assets from theft.

Biometric systems have advantages for employees as well. For instance, employees no longer have the need for access badges, keys, or parking passes. Additionally, their identity cannot be stolen and used by someone else.

Normally this technology is stored in a database as a mathematical template of a fingerprint and is perfectly secure. However, there are advanced systems that allow employees to retain control of their template. Instead of having the template stored in a company database, it is stored on a smart card's chip. When employees want to gain access to a facility, they present/use their smart card in addition to their fingerprint. The reader matches the fingerprint to the template stored on the card. This is a very secure system because even if a card is stolen, no one can gain access to a facility using it since his or her fingerprint will not match the template stored on the chip. Additionally, no one can modify the template because the information stored on the card is encrypted.

SECURITY TECHNOLOGY IN DAY-TO-DAY OPERATIONS

Along with the development of new biometric technologies, progress has also been made in more traditional areas of safety/security technology over the last few years. Such technological advancements improve existing safety/security measures and increase their overall effectiveness. The following are a few examples:

- electronic field data capture in highway patrol vehicles
- advanced wireless communication technologies that allow easy access and exchange of data during major events or in case of emergencies
- electronic data capture and processing
- wireless location identification technology (known as wireless enhanced 911)

- real-time in-vehicle route guidance systems that enable emergency vehicles to move more efficiently through congested roadways
- innovative surveillance technologies to help monitor traffic violations and activities in public areas
- secure networking and online communication and sensitive data exchange using Virtual Private Networks (VPNs) and data encryption
- Internet crime prevention tools that allow law enforcement to update communities about crimes in the area, severe weather, bomb threats, or other important matters