November 2000

Biometrics and Network Security

Norman Desmarais
Providence College, normd@providence.edu

Biometrics and Network Security

Norman Desmarais

Theft of identity is becoming the nation's leading incidence of fraud. Yet we continue to transmit purchase orders and other private messages over unsecured telephone lines via e-mail in ASCII text, which is the least common denominator for electronic text. We rely on passwords, cards, personal identification numbers, and keys to access restricted information or confidential files. But these forms of identification can be forgotten, stolen, forged, lost, or given away. Moreover, these devices serve primarily to identify the person. They cannot verify or authenticate that the person really is who he or she claims to be. Many systems rely on IP address verification that limit access to users with a specific domain name or Internet address. Basically, this procedure identifies an individual by the machine he or she uses. Anybody using a particular computer can impersonate the rightful owner.

Biometric devices are emerging as more viable means of protecting personal security. Biometrics, which means "life measurement," is based on the principle that everyone has unique physical attributes that, in theory, a computer can be programmed to recognize. Biometrics uses mathematical representations of those unique physical characteristics to identify an individual or to verify identity. It can serve to authenticate people because everyone has unique and somewhat stable body features and ways of doing things. While passwords, cards, personal identification numbers, and keys can be forgotten, stolen, forged, lost, or given away, biology can't be.

Biometric techniques fall into two categories: physiological and behavioral. We shall take a brief look at the techniques used in these two categories and consider some of the applications for biometric technologies. Common physiological biometrics include finger characteristics (fingertip [fingerprint], thumb, finger length or pattern), palm (print or topography), hand geometry, wrist vein, face, and eye (retina or iris). Behavioral biometrics include voiceprints, keystroke dynamics, and handwritten signatures.

Physiological Biometrics

Finger/Hand

Fingerprint technology is the most commonly used biometric because it has been used in law enforcement for over a hundred years. However, prisons and law-enforcement populations are comprised mostly of relatively uniform populations of males between the ages of 18 and 36 whose fingerprints are in relatively good condition. Some people have fingerprints that are harder to image. About 2% of the general population's fingerprints baffle computers. It's often difficult to image fingerprints from people with very small hands and fingers, people who work with their hands, or those who have injuries or scars. Also, as people age, they often lose the lipid (fat) layer in their skin and their fingerprints become worn and difficult to image.

Fingerprint scanners could work fine in a private security application where it may suffice to match a few locally stored prints. They are more difficult to fool than face-recognition systems because they measure the unique and complex swirls on a person's fingertip and some can even accommodate cuts. However, a public security setting, where potentially anyone's prints would need to be matched, could pose problems because current methods require large central databases. For example, if a customer makes a purchase with a credit card, his or her fingerprints might have to be matched against everyone who owns that particular card unless there is a tamper-proof way of storing prints locally. Also, cuts and dirt can distort images. If a previous user leaves an oily latent image on the scanner, a false rejection may occur or someone with a fine brush and dry toner could "lift" fingerprints with adhesive tape.

Palm/hand scanners, a variation of the fingerprint scanners, are better suited to sites in which the users may be working with their hands. They measure creases and/or geometry that will not be substantially altered by grime or nicks. However, these devices are also more expensive and less accurate than the fingerprint scanners, especially at sites with a large number of users.

Some manufacturers rely on smart cards to control access, particularly to notebook PCs. They encode fingerprint data (128 to 512 bytes) in the smart card's microprocessor; it operates like a bank cash machine where one enters the card and a personal identification number (PIN).

Face/Eye
Face recognition also satisfies most of the criteria for the ideal biometric solution. It's easy to perform, fast, moderately convenient, and nonintrusive, except perhaps to the camera-phobic. Video camera hardware is relatively inexpensive; and some monitor manufacturers build camera lenses into their display screens to accommodate videoconferencing. With todayís faster processors, even a low quality digital camera can do a pretty good job of reading digital video and can recognize individuals 78 percent of the time. These factors contribute to making face recognition one of the fastest-growing niches. However, the technology is subject to spoofing; and lighting can affect authentication.

Face-recognition systems can also work with people still at a distance. As one approaches, the system could recognize the face and activate the system, such as turning on a computer or unlocking a door.

Some applications are focusing on a person's smile as a replacement for a security password. Other techniques based on ear or lip shape and knuckle creases are in the conceptual stages; and one startup company is trying to recognize a person's identity by body odor.

Eye scanning is probably the fastest growing area of biometric research because of its promise for high scan accuracy and great difficulty to fool. There are two types of eye scanning: retinal scanning and iris scanning. Retinal scanning uses lasers that focus on the back of the eye, while iris scanning zooms in on the front. The retina is considered unique even among identical twins. Likewise, the iris is the most feature-rich part of the human anatomy that is constantly on view. The iris can have more than 250 distinct features, compared with 40 or 50 points of comparison in fingerprints; so iris scanning is an order of magnitude more accurate than fingerprints or even DNA analysis. Also, unique patterns in the human iris stabilize within one year of birth and remain constant throughout one's lifetime, unlike other biometrics. However, contact lens wearers or people with optical diseases like glaucoma may ! ! not easily pass an eyeball scan. It is also impossible to counterfeit the distinct iris pattern with any existing scientific technology.

Behavioral Biometrics

Behavioral biometrics cost the least to implement; but they are less robust than physiological ones. The most promising methods today include voice recognition, keystroke dynamics, and digital signatures.

Voice recognition is the second most secure method after eye scanning; but it is less secure and the process is slow and subject to a person's physical or emotional state. The systems used for security operate in much the same way as voice recognition (discrete commands) and speech recognition (continuous speech) systems and are generally used in combination with PIN numbers to act as a password to keep systems secure. Some people worry that the voice can be recorded and played back for identification. Others think that the threshold might be too low, resulting in access systems nearly as complicated as the password approach.

Keystroke dynamics is a technique that monitors a user's fluctuating typing speed patterns. It identifies people by their unique typing rhythm, i.e. the length of time they spend pressing keys and moving their fingers around the keyboard. People move their fingers in precise, yet irregular, timing patterns during log-ins without realizing it. Even when somebody knows another's password and listens to that person enter it, one cannot imitate the keystroke speed fluctuations precisely. Keystroke dynamics have not yet found their way into commercial use, primarily due to legal questions. The issues involve personal privacy and whether a company might use such techniques to monitor the hourly progress of its employees.

Digitizing tablets can also be used as biometric devices for authenticating network users. Signature technology has a large advantage over most other behavioral biometrics because a signature is traditionally used in authorizing legal documents, bank transactions, personal file access, and so forth; but it can also be subject to a person's physical or emotional state.

Applications

Biometric devices have a bright future. Proponents foresee their use in ATMs, access control door security, computer security, and time clocks. Optimists foresee passports, drivers' licenses, mortgage loan applications, health records, safety deposit boxes, credit card transactions, e-commerce, drug distribution, lottery tickets, and prisons as other application areas.

Biometric technologies are relatively inexpensive, requiring little or no new hardware and nothing more than commonplace actions. This makes them attractive, especially in situations where remote users must be supported. However, more universal implementation at the desktop or workstation level will require prices to drop even further. It may require prices to drop to the $5-$10 range before consumers and employers adopt this technology. Even such low costs represent a sizeable expenditure for large organizations. Cost becomes an even more important issue when one does not rely on a single security device but couples two different techniques for greater reliability.

The ideal biometric would be easy to use, fast, non-intrusive, convenient and socially acceptable. Most biometric technologies are computationally intensive and some users see biometrics as an invasion of privacy. Biometric techniques involve trade-offs among several factors, such as accuracy, ease of use, cost, and user acceptance. While security experts may cringe at the thought of passwords, the losses from potential security breaches are usually lower than the price of biometrics, considering the purchase price, configuration cost, and inconvenience factor.

Library Applications

One only needs a microphone or camera, a fingerprint or eye scanner, and the corresponding software to begin working with biometrics; but biometric devices are probably overkill for most library applications. However, they may become important tools to gain access to institutional computers. IT managers may adopt them to protect access to sensitive information, such as personnel records, salary and medical information, and academic or disciplinary records. Researchers may want to have biometric devices installed to block unauthorized access to research findings, dissertation work, or research conducted under government or foundation grants.

Librarians, among others, may be more interested in protecting the privacy of their electronic communications or in protecting the integrity of the content of the resources they provide. Library catalogs and electronic resources are exposed to increasing risks of tampering by the general public. Moreover, librarians are licensing more and more electronic materials. As license (i.e. contract) administrators, they may be held accountable for the use of those materials and be liable for contract infringements.

Biometric devices may find their way into library applications as publishers, aggregators, and electronic information providers attempt to restrict access only to authorized subscribers or licensees. Instead of having to manage ranges of IP addresses or a list of valid user names and passwords for a variety of products or publishers, license administrators may find themselves managing a list of biometric codes and devices.

Summary

Network security demands attention at multiple levels. Still relatively expensive and immature, biometric technologies vary in accuracy and reliability. At this point, they may be most effective when used in tandem with other security measures.

Biometric Information Sources

Biometric Consortium
http://www.biometrics.org
This is the U.S. government's biometrics site. It contains publications, research, databases, events and government activities.

International Biometric Group
http://www.biometricgroup.com
This site contains biometric news and consulting and offers information free or by subscription.

International Computer Security Association
http://www.ncsa.com
This site contains information on security and cryptography.

Bibliography

Brown, Chappell. Self-contained Fingerprint IDs *Forgo PCs, Networks. Electronic Engineering Times*, Dec. 14, 1998 p 61.

Dawley, Heidi. A Program That Never Forgets a Face. *Business Week*, Dec. 21, 1998 p81.

For Your Eyes Only: Biometrics. *The Economist*, Feb. 14, 1998 v346 n8055 p80.

Hooman Bassirian. Passwords Could Be Past Tense by 2002. *Computer Weekly*, November 26, 1998.

McCooey, Eileen. Security Becomes a Priority. Compaq, Dell, others adding security hardware to PCs. *Windows Magazine*, January 1, 1999.

Phillips, Ken. New Options in Biometric Identification. *PC Week*, Sept 7, 1998. v15 n36. p95.

Phillips, Ken. Not everybody's HA-API. *PC Week*, Feb 2, 1998. v15 n5. p95.

Surkan, Michael. Biometrics: All the Way or Not at All; implementing new security technologies.*PC Week*, December 7, 1998.