Global Information Assurance Certification Paper

Biometric Security -Practical and Affordable!

Timothy Greene

January 17, 2001

INTRODUCTION:

Once the stuff of James Bond movies, biometric security devices--scanners that read your fingerprints, cameras that recognize your face, software that knows your voice--are in use and readily available. Upon research, one can determine that biometric products are not just dreamware…they are practical answers for serious security challenges. As a result, the purpose of this paper is to discuss biometrics as an affordable and favorable layer of security protection for the consumer; and concerns about biometrics that relate to privacy issues and compliance standards.

DEFINITION:

Biometrics can be defined as measurable characteristics of the individual based on their physiological features or behavioral patterns that can be used to recognize or verify their identity. Biometric technologies attempt to automate the measurement and comparison of such characteristics for recognizing individuals. Many different technologies have recently been developed for person recognition and identity authentication. Some examples include measures based on information from handwriting (especially signatures), fingerprint, face, voice, retina, iris, hand or ear shape, and gait data.

USE IN BUSINESS:

Biometric technologies were first proposed for high-security specialist applications but are now emerging as key elements in the developing electronic commerce and online systems revolution, off-line and standalone security systems, and as well as for personal computing protection. These technologies provide important components in regulating and monitoring access and presence. Significant application areas include electronic commerce, security monitoring, database access, border control and immigration, forensic investigations and telemedicine.

The development of biometric technologies, beyond traditional high-security applications, has a compelling financial motivation. Transaction security is critical to e-commerce's future development and there is serious concern over the adequacy of current solutions. The concerns with personal identification numbers, PINs, and identity tokens, such as cards, are that they do not guarantee the identity of the person who uses them. Credit card fraud has been reported to cost over 500 million dollars per year and ATM fraud has been reported as high as 3 billion dollars. Biometric systems have the advantage that they are tightly bound to the individual and can not be easily used by an impostor.

In addition to such verification applications, biometric systems can be used for the less constrained problem of automatic identification of individuals. In this mode, the biometric system carries out a "one-to-many" search of its stored models of individuals' identities. As a result, the biometric systems can be used in security applications, such as fraud and/or intrusion detection.

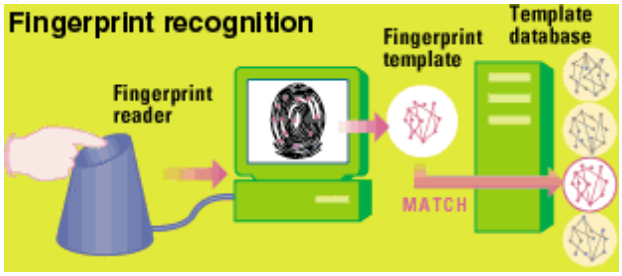
USE IN SOHO AND PERSONAL COMPUTING:
Originally designed for large companies, biometrics have now been scaled and made affordable for small networks and stand-alone systems. For example, the vendor market has the following biometric applications/hardware available for purchase:

- $100 - will buy a digital face recognition software with a five user capacity
- $100- will buy a voice recognition software to recognize and authenticate your voice pattern and apply the verification process to grant access to telephone and network systems
- $150 – will buy a fingerprint scanner on PC card that can replace passwords on your favorite Web sites, applications, and even fill out personal information on user selected Internet forms.

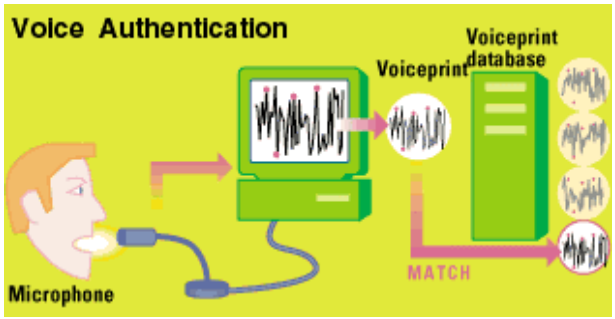
Biometric systems go a crucial step beyond traditional passwords or security-access cards, also called smart cards, by ensuring that the individual trying to log on is actually the authorized person--not just someone who found a key card in a desk or the Post-It note with a password under the keyboard. Biometrics' use a person's unique physical characteristics as a means of verifying a person's identity and thus grant--or deny--access to computer resources.

No matter what biometric method you use, the underlying process is similar: To enroll a new user, you must store an encrypted template file of the user's biometric information on a server or client PC. When the user logs on, the template is compared against the new, live information. If it checks out, access is granted. See examples below:

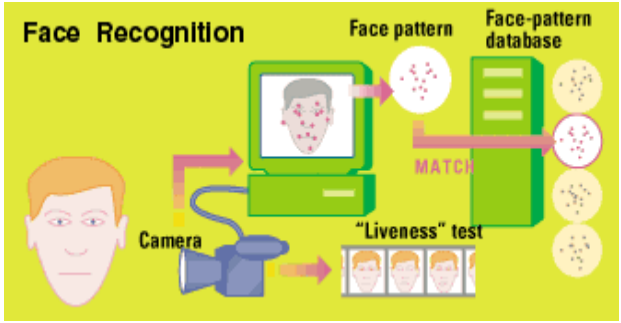
Fingerprint-recognition packages scan your finger from several angles and store the template on a server or local hard disk



Voice-authentication products create a voiceprint based on the inflection points of your speech, emphasizing the highs and low specific to your way of talking.



Face-recognition software uses a camera attached to your PC to capture and map key identifying features. Some also perform a "liveness" test to see how your face moves, so that a photo of you cannot be used.



Iris-recognition technology using an Authenticam (computer-tethered camera) that takes pictures of a person's iris from a distance of 18 to 20 inches. The image is then analyzed and generates a 512-byte code, half of which is content. The code is compared with the iris imprints in a database and used to determine the individual's authorization level. Industry claims that the whole process takes only 2 seconds, even using a very large database of imprints.

The extra security that a biometric system offers is important with regards to Extranets, remote-access devices, and VPNs (virtual private networks), which provide access to companies' or individual's private and sensitive data at points behind the corporate or personal firewalls.

However, let's not forget that biometrics is not just about security, it's about convenience; forgotten passwords and lost smart cards are a nuisance for users and eat up a lot of expensive Information Technology (IT) time.

COMPARING THE PLAYERS:
Products that rate well in desktop setup are easy to deploy on client desktops. Ideally, biometric products serve a larger audience if they:

- Require minimum hardware requirements and a straightforward software installation.
- Provide a seamless Windows NT integration and cross-platform support (NetWare, Windows NT, and flavors of Unix) are pluses.

In addition, in an enterprise/network environment, biometric solution providers should include the following:

- A better rating in enrollment which would facilitate adding new users quickly and with minimum intrusion (especially important for large-scale deployment).
- A centralized enrollment database is preferable to one that forces users to enroll on each machine they might need to use. Remote enrollment capability is a plus.
- Total cost of ownership (TCO) with considers a system's setup-front costs, the time and resources a product's deployment would demand and the impact on employee productivity (how easy a system is to use day in, day out).
- Provide robust administration tools and flexible setup options for network. For security, products that offer administrator-definable sensitivity thresholds and centralized, encrypted databases are favored best. The option to integrate the system with smart cards or passwords is always a plus.

With regards to the last bullet, you might think that your fingerprints, face, or voice remain constant from day to day, small fluctuations (cold or moist hands for fingerprint scanners, different ambient lighting for face recognition, and background noise for voice authentication) can stymie the devices. Setting the sensitivity lower makes the product more forgiving but increases the odds of a false positive--a faker logging on as someone else. Higher sensitivity means greater security, but it also means that an authorized user may be erroneously rejected (false negative).

PERFORMANCE FACTORS:
An important issue for the adoption of biometric technologies is to establish the performance of individual biometric modalities and overall systems in a credible and objective way.

For verification applications, a number of objective performance measures should be used to characterize the performance of biometric systems. In these applications, a number of 'clients' are enrolled onto the system. When being verified, the clients should be recognized as themselves and impostors should be rejected.

Another important performance parameter is the verification time defined as the average time taken for the verification process. This may include the time taken to present the live sample.

While some vendors quote the False Acceptance Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER) performance parameters for their system under laboratory conditions, there are seldom real world performance characteristics available for biometric systems. This is because it is almost impossible to account for the complexities of all possible real world conditions. For example the actual verification time will critically depend on user training, operating environment and psychological conditions such as stress. As a result, vendor specifications should be seen only as rough guides to real world performance.

- FAR - the ratio of impostors that were falsely accepted over the total number of impostors tested described as a percentage.
- FRR - the ratio of clients that are falsely rejected to the total number of clients tested described as a percentage.
- EER - the threshold level for which the FAR and the FRR are equal. It is often quoted as a single figure to characterize the overall performance of biometric systems.

CONSIDERATONS:
In addition to the performance factors, the biometric sector must be very cautious when dealing with the important issues and considerations as stated below:

Acceptance: Biometric technology must be easy to use during both the enrolment and comparison phases. It must be socially acceptable and not have the appearance to threaten user's privacy and confidentiality or appear to treat the user as a suspect or criminal.

Integration: The hardware platform on which the system is to be implemented is a key concern. The software, hardware, and networking requirements should ideally be compatible with existing systems, allowing the biometric system to be integrated to the existing infrastructure. The system cost should be reasonable and the maintenance costs should be understood.

Legal: There are still concerns over potential intrusions into private lives by using biometric systems. The legal issues must be considered for any potential application and appropriate measurement is taken. For instance, the Euro-community's comprehensive privacy legislation doesn't specifically mention biometrics, however, the overall concerns and chance for of a legislative challenge remains active.

Robustness: In addition to systems being robust enough to accurately detect fraud and impersonation, they should also be adaptive to handle small variations to the users' biometrics over time.

Speed and Storage Requirements: The time required to enroll, verify, or identify a person is of critical importance to the acceptance and applicability of the system. Ideally, the acceptable verification time should be of the order of one second or faster. The storage requirement for the templates is also an important issue, especially if the templates are to be stored in magnetic stripe or smart cards.

BIOMETRICS IN USE TODAY:
The combined and simultaneous use of audio and video information provides a greater degree of security as tampering any one of these sources would not be enough for false access and authentication. Joint audio-visual models for individuals may be encrypted and placed on smart cards and used for authentication and controlled access to buildings and resources.

With the increasing availability of desktop video-conferencing and the decline in the price and availability of multimedia video capture and processing equipment, the use of joint audio-visual processing for authentication and access control is feasible and cost-effective.

For fingerprint recognition products, tests (such as dusting for latent prints on the device, lifting them with tape, and reapplying them to the reader) were unable to fool the devices. The lack of success using the lifted print test is a reflection of the relative maturity of fingerprint recognition technology, which has been in use in a number of environments for decades.

The table below lists the more common biometric sources of identity information and key characteristics of some current systems; classified in broad terms:

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	Low
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	Medium	Medium	Medium
Signature	Medium	Medium	High
Face	Low	High	High

From a 1997 report done by the University of Athens

CONCLUSIONS:
As for cost, the jury is still out. In a stand-alone or SOHO scenario, there appears to be moderately priced biometric solutions. The current generation of biometric identification devices offers cost and performance advantages over manual security procedures.

On an enterprise-wide scale, IT and finance management will have to determine if the price per seat will be cost effective and made up for in fewer calls to the Help Desk and a more productive workforce. Unfortunately, companies will have to pilot test (preferably prior to purchasing) the biometric devices and see if using the products will truly decrease the total cost of ownership.

No single biometric has dominated the market. Different technologies are used for the same applications. The current need in the biometric identification field is to have the market make greater use of what already exists.

Careful evaluation of all mathematical tools (algorithms, protocols), software involved in the biometric technologies should be performed.

The security strength of the biometric methods should be proven. In particular the biometric methods should be tested against any cryptanalytic attack. As the computer power grows, theoretical attacks that are not feasible with the present computing power, will be successful in the near future. As a result, research should be undertaken by institutions whose expertise is to test the vulnerability of security systems.

The claims of systems designers need to be assessed by independent evaluators. The establishment of evaluation centers will bring the confidence that is missing today. An independent screening testing of all devices should be performed, i.e. treating the biometric devices as black boxes to examine how well the devices perform. These tests should be performed by independent institutions where manufacturers are not involved.

One of the biggest problems facing early adopters of biometric technology has been dealing with non-standardized error-rate reporting for FRR and FAR (false rejection rate and false acceptance rate), which mislead buyers about the suitability of a product. Once standards are invoked, then biometric technology will show evidence of reliability. Standards will also help manufacturers to evaluate their biometric products against certification tests and provide potential buyers with level of assurance and comfort through compliance.

References:

[1] Gustafson, D. "Biometrics: Has its time come?", October 31, 2000, http://www.sans.org/infosecFAQ/authentic/biometrics_time.htm

[2] Association for Biometrics (AfB) and International Computer Security Association (ICSA), "Glossary of Biometric Terms", http://www.afb.org.uk/public/glossuk1.html, 1998

[3] Best Practices in Testing and Reporting Performances of Biometric Devices, Version 1.0, 12 January 2000, Biometrics Working Group (UK), http://www.afb.org.uk/bwg/bestprac10.pdf

[4] Newbytes, "Low Cost Shrink-Wrapped PC Biometrics At Last", December 9, *1999*, http://exn.ca/Stories/1999/12/09/04.cfm

[5] Phillips, K., "Standards Coming to Biometrics Market", PC Week Labs, May 22, 1998, http://www.zdnet.com/eweek/stories/general/0,11011,317809,00.html

[6] Phillips, K., "Unforgettable Biometrics", PC Week Labs, October 29, 1997, http://www.zdnet.com/eweek/reviews/1027/27bioapp.html

[7] Dr. Polemi, D., "Biometric Techniques: Review And Evaluation Of Biometric Techniques For Identification And Authentication, Including An Appraisal Of The Areas Where They Are Most Applicable", April 1997.

[8] Deravi, F., Audio-Visual Person Recognition for Security and Access Control, http://www.jtap.ac.uk/reports/, January 9, 1999