



# BIOMETRICS

## A logical choice for logical access?

By Ms. Michelle Dugan

Air Force Communications Agency

**SCOTT AFB, Ill.** — Pretend you're sitting in your favorite recliner watching a spy movie. On screen a secret agent is stealthily attempting to enter the enemy's computer facility. He's there to steal secrets, but he needs one of the enemy's index finger prints to log in to the computer.

The agent coolly touches the fingerprint reader wearing a latex version of someone else's fingerprint. He successfully logs in and gets the information he needs to change the coordinates of a nuclear warhead. Sound far-fetched?

Not really.

Today, biometric technology, which uses unique biological identifiers every person possesses, is being used in a variety of applications.

However, biometric fingerprint readers on the market do test the finger for life signs to prevent the scenario above from actually occurring. To some people working within the realm of information assurance, biometric technology may appear to be a future concept, a reality looming on the fringes of programs such as Public Key Infrastructure or common access card. However, biometrics used for authentication to computer networks or systems, also referred to as logical access, is undergoing testing in the

Department of Defense and is already implemented in many commercial and government facilities.

With respect to logical access, biometric technology is used to augment or replace UserIDs and passwords, enhancing the security of authentication from something someone knows to something they are, which cannot be lost, forgotten, or easily stolen. Is biometrics a logical choice for logical access?

### BIOMETRIC TECHNOLOGY

Biometrics is automated methods of identifying or authenticating a living person based on a physical or behavioral characteristic. Examples of biometric technologies that measure physical characteristics include fingerprint and iris scans, hand geometry, and facial recognition. Technologies that measure behavioral characteristics include signature verification and voice recognition.

Biometrics can be implemented as an authentication tool, referred to as a 1:1 search, where a user's biometric known template is compared against a database. Biometrics can also be used for identification, referred to as a 1:many search, where a user's unknown biometric template is searched against a database to identify that individual. An example of identification could be a

facial recognition biometric device installed at airport security to scan faces in the security line and search for matches of "persons of interest" loaded in a biometric database. However, this is an example of applying biometric technology for physical security, instead of logical access to computer networks or applications.

### UNDERLYING ISSUES

Tests that have been conducted on biometric technologies have included the False Reject Rate, which indicates the rejection rate of those users enrolled in the biometric that should have access, but are denied. This data is important in environments where positive access to the controlled area or system is paramount.

But perhaps more importantly, from

For questions on biometrics or biometrics requirements, contact AFCA/WFP at DSN 779-5260 or visit the Air Force Communications Agency Biometrics section under Info & Services on the Air Force Information Assurance Web site:

[https://private.afca.af.mil/ip/info\\_services/ca\\_info.cfm](https://private.afca.af.mil/ip/info_services/ca_info.cfm)



an information assurance perspective, is the False Acceptance Rate. That indicates the acceptance rate of users who are not enrolled in the biometrics that should not have access, but are authenticated. The FAR is difficult and often not feasible to measure on a comprehensive scale because what's needed is a large sample size of users not enrolled to test out the device to ensure access is not granted.

While security is a preeminent concern, users are also interested in how their biometric data will be protected. Currently, the amount of biometric data traversing the network is minimal. However, this is expected to increase in the future, while measures to minimize potential risk for exploitation and protection of data in transit and on storage services are still being researched.

### IDEAS ON HOW TO IMPLEMENT

Implementation of biometrics for logical access is still in the testing phase. However, the deputy secretary of defense outlined an enterprise vision for biometrics in August of 2003.

“By 2010, biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for logical and physical access control.”

While the DOD and Air Force level policy and guidance is still in the

developmental phases, there is a clear sense that biometrics is the way ahead for providing increased information assurance.

Dr. John Woodward, director of the DOD Biometrics Management Office, recently conducted interviews with senior leaders from different military and government services on their perspectives on biometrics.

Perspectives on the benefits of biometrics for logical access included increased authentication and non-repudiation, monitoring insider threats or unauthorized use, potential cost savings when compared to maintaining UserIDs and passwords.

On the other hand, is there truly a requirement for biometrics as an added layer of security in addition to PKI or CAC, and what are the error rates for various biometrics technologies?

The Air Force Communications Agency, as lead command for Air Force biometrics, has an integral role in collecting and advocating biometric requirements from the field and working closely with the DOD biometrics management office on testing, standardization, and policy efforts.

Once this foundation is laid, biometrics appears to be a logical choice for logical access, another layer of security to protect critical information systems.

**Biometric technologies measure physical characteristics that include fingerprint and iris scans, hand geometry and facial recognition. Technologies that measure behavioral characteristics include signature verification and voice recognition.**