



"Authentication is something you have, something you know, and something you are when you add biometrics"

Charles Kolodgy, Research Manager,
IDC, Framingham, MA. InfoWorld, January 2001.

Biometrics: You Are Your Own Key

Authentication is the process of identifying an individual. Traditional authentication methods are based on passwords and tokens. The problems with these techniques arise when the passwords or tokens are lost, stolen, or misplaced, which eventually leads to fraudulent incidents. For instance, someone can misuse your stolen network password to gain access to confidential information.

A reliable solution to these authentication problems lies in biometrics. Because biometrics does not rely on any passwords or tokens, there is no question of anything being lost, stolen, or misplaced.

What is Biometrics?

Biometrics refers to the automated identification of a person, on the basis of physiological and behavioral characteristics. The physiological characteristics could be face, fingerprints, hand geometry, handwriting, iris, retinal etc. Examples of behavioral characteristics are voice, signature, body odor etc. Identification based on these characteristics is more reliable and distinctive, as these characteristics mostly remain stable and unalterable. One can very well say that the "Key" for entry into a biometric system is "You" the individual.

How does it work?

There are two distinctive operational modes of biometric technology – Identification and Verification. Identification relates to establishing the identity of a person as in "Who am I?" On the other hand verification relates to verifying the claim "Am I who I claim am I?"

The first activity to enable the use of a biometric system is the enrollment process. During enrollment, biometric characteristics of individuals are measured and stored in a repository. During verification, the system acquires the biometric patterns using a sensor, filters the information to a standard form, issues a search query to the repository, then a decision is made whether the pattern has been found or not and finally an output response is generated. If the pattern is found in the repository and matches, the system verifies the person successfully. Otherwise the person is trying to break into the system as an impostor.

Present Scenario

Biometric technologies have long been in use for forensic activities. In the past few years biometrics have been deployed in banking, airport security, network authentication, hospitals, retail stores etc. Examples include:



- BankUnited (now Washington Mutual) had introduced Iris scan technology in some of their ATMs in 2000. Ninety-Eight percent of users were positive about the experience, citing it as more secure, convenient and more reliable than regular ATMs.
- Facial recognition systems to detect criminal and terrorist intrusion are being pilot tested at Dallas/Fort Worth and Palm Beach international airports.
- The Health Insurance Portability and Accountability Act (HIPAA) recommends the use of biometric technologies to provide secure access to patient records. The patients can identify themselves securely and efficiently in this way.
- West Seattle Thriftway, a grocery store in Seattle, Washington uses fingerprint biometrics to link customers to their credit cards or bank accounts. The system amounts to savings up to \$50,000 annually for the owner and also leads to convenience and speed of operation for the store customers.

Future Outlook

Looking at the market, according to the International Biometric group (Biometric Market Report 2001), Biometric revenues are expected to grow from \$399.4 million in 2000 and \$523.9 million in 2001 to \$1.9 billion in 2005. Large-scale public sector biometric usage, currently 70% of the biometric market, will be surpassed by private sector deployments.

Biometrics has a myriad of applications in various commercial sectors. The technology offers a secure means of identification and authorization. It saves time and money, is convenient, and makes the world a more secure place.

Picture this hi-tech corporate office scenario. You enter your office and within no time, the video camera on top of the door scans your eye's retina, verifies it, and opens the door for you. You go in front of your computer, say "Hello" and the system powers up, and automatically logs you in your account. Biometric technology can open lot many doors like these. The benefits are tremendous - no human surveillance, money and resource savings, and no reliance on memory.

Imagine another situation – You have to go and watch a baseball game, you walk into the sports stadium, enter the gate, you are identified using the retinal scan, you state the ticket you wish to buy. Your bank account is charged automatically, your seat number is displayed and you move in to the stadium.

We can very well foresee similar kind of applications in shopping malls and retail stores that will use fingerprint or any other biometric for identification.

The next generation of vehicles will not require any keys to open or start. They will use your voice as an identifier. The vehicles would store profile information for the drivers. The driver



just needs to identify using a biometric and the preferences of the driver (related to mirrors, seats, etc.) would be set up automatically.

Issues and Challenges

Biometrics is not a cure-all technology per se. The issues and challenges that need to be addressed include the following:

Accuracy

Even with a legitimate biometric sample one cannot be sure whether authentication will be successful or not. Various factors like noise, processing methods, and variations in representation play a significant role.

Forgery

"Everything in the world can be faked if you have enough time and money," says Biometric Access CEO Ron Smith. "But it's a whole lot tougher to fake a fingerprint than to steal a password. So what you're doing is raising the fortress wall." In contrast to Ron's statement however, Tsutomu Matsumoto, a Japanese cryptographer, has found a way to fake fingerprints. This is a big concern that needs to be addressed. Controlling "Identity Theft" will be a huge challenge.

Infrastructure and Cost

Biometrics systems are currently price prohibitive. The costs are related to hardware, software, and deployment. However, with mass scale adoption and manufacturing of biometric devices, cost can be substantially reduced. If we perceive having universal biometric IDs then there is a major issue related to the repository – whether the repository will be centralized or distributed, how it will be accessed, what kind of security measures and so on.

Privacy

With the individual being tracked everywhere, biometrics are inevitably compared with "Big Brother" by critics. There are legal, ethical, and policy concerns that need to be addressed.

Standardization

There are diverse biometric technologies that can be integrated into a variety of applications. Currently, each of the providers of biometrics use their own standards. The integration standards need to be defined for the technology to prosper. There are bodies that are pushing for convergence of these standards. The BioAPI Consortium is promoting application integration across numerous biometric systems. The National Institute of Science and Technology (NIST) is promoting the development of a common format for exchanging templates among biometric systems (Common Biometric Exchange File Format: CBEFF standard).



Summary

Biometrics finds applications in access control, forensics, e-commerce, retailing, criminal screening at airports, etc. Apart from providing secure access to resources and information, biometrics are convenient and efficient. The key issues that need to be resolved for global adoption of the technology are accuracy, forgery, infrastructure, cost, privacy, and

standardization. The time is not far when biometric technologies will come out of the realm of science fiction and become part of every day life.

Vinay Ahuja

vxa010400@utdallas.edu

Additional Readings and Sources

1. Avanti Biometric Reference. <http://homepage.ntlworld.com/avanti/home.htm>
2. Biometric Digest. <http://www.biodigest.com>
3. Biometrics Technology Today. <http://www.biometrics-today.com/>
4. Biometrics Consortium. <http://www.biometrics.org/>
5. Biometrics links at Network World Fusion.
<http://www.nwfusion.com/research/biometrics.html>.
6. Biometrics Research at Michigan State University.
<http://biometrics.cse.msu.edu/index.html>