Biometrics: Face Recognition Technology
Veronica Henry
March 12, 2001

> "The word "biometric" simply means the measurement of a living trait, whether physiological or behavioral. Biometric technologies compare a person's unique characteristics against a previously enrolled image for the purpose of recognizing them, similar to the way our brains identify each other, but on a lesser scale."

Network Security

With the expansion and globalization of corporate networks and the added presence of internet connectivity, network security has become one of the biggest concerns facing today's IT departments. It has become increasingly difficult to manage these external connections in a safe and secure manner.

Additionally, with the advent of mobile workers, wireless devices and always-on internet connections, we are further challenged with finding a way to take advantage of all the recent technological advancements while ensuring safety and privacy of information.

These changes may lead us to ask the question - Why aren't networks secure? For starters, there is increased usage of shared network infrastructures, long standing SNMP management system vulnerabilities, highly developed infiltration tools and a sophisticated hacker community.

Then we may ask - What do we need to do? Basically we need to protect data, resources and corporate reputation.

The only way to address these issues is to develop and implement a sound security policy and follow-up with periodic auditing of these policies.

Authentication

The process of identifying an individual is usually based on two things, a username and a password. Authentication merely ensures that the individual is who he or she claims to be, and does not address the issue of access rights. Network administrators might be more familiar with the term authorization, which is the process of giving individuals access to a system based on their identity.

Referencing the paper by Allison Miller, there are three methods of authentication:

- Something the user knows (user name, password, pin)
- Something the user has (i.e. Tokens, ID Cards, smartcard)

- Something the user is (i.e. Voiceprint identification, retinal scan, face recognition)

Authentication by username and password is more likely to be compromised. We need additional authentication methods in order to ensure security.

Biometrics Technology

Biometric technology seeks to improve upon basic password authentication via voiceprint, facial scan, retinal patterns and fingerprints. While still not in wide adoption today, advances in hardware and software, combined with reduced pricing have made biometrics a more viable authentication option in today's corporate networks.

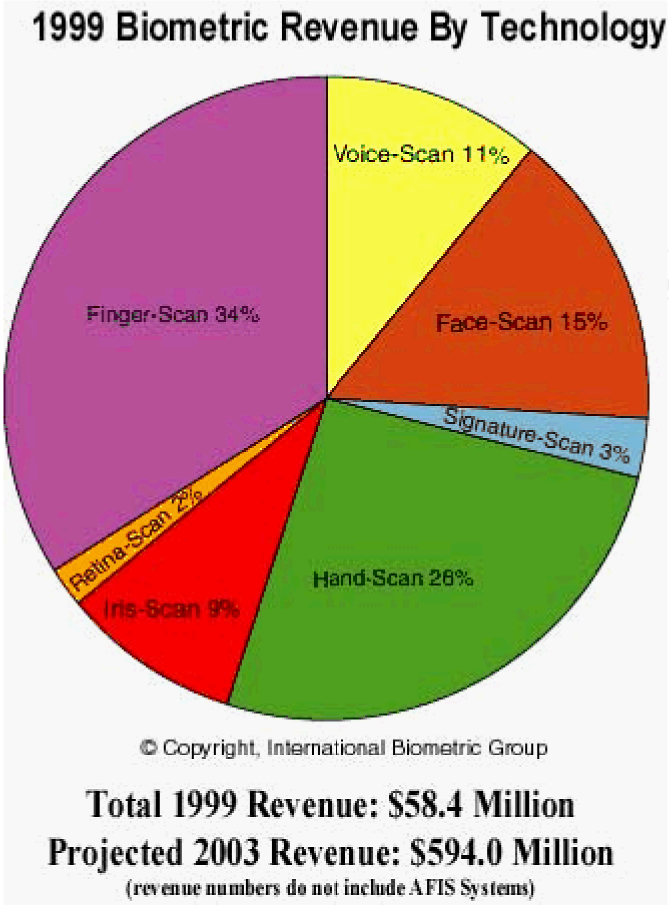
Two of the main reasons for the slow adoption of biometrics is cost and lack of standards. Several standards proposals are in development. In particular, HA-API (Human Authentication API) and BAPI (Biometric API). HA-API (released in 1997) provides a means to interface to various biometric technologies, but only under the Win32 platform. BAPI, under development by the BioAPI Consortium, provides an OS-independent standard and makes the API biometric-independent.

Beyond the lack of firm standards, biometric technology still struggles with lack of trust and recognition from end users. While those who work in the IT arena will at least have heard of biometrics, the user community at large is unaware of this technology. Many associate fingerprint scanning with the fingerprinting of alleged criminals and are hesitant to accept this technology. Others have concerns about potential abuses of the data collected via these systems. Consequentially, until end users are comfortable with this technology there will be resistance to it's use. Systems administrators required to support this technology will also need additional platform, auditing and systems management support as well. These issues are being addressed by software vendors, but aren't readily available.

Biometric systems aren't meant to be replacements, but rather an addition to the existing authentication scheme. Most networks maintain a combination of authentication technologies, deemed "two-factor" authentication. This should be kept in mind when designing a biometric solution, you will need a model that will integrate with your existing technologies in the future. Products that best accomplish this integrate existing technologies (such as smart cards) with biometrics and establish a management interface that allows for the addition of modules to support new technology. Shops that are in good shape for biometrics will have a largely homogeneous Windows NT platform with an authentication system that is primarily password-based. Larger shops may be able to integrate biometrics into specific applications or for some users as the market develops.

Different biometric technologies are better suited to certain industries or applications. As you might expect, fingerprinting (currently the largest revenue generator, fig. 1) and eye scanning are popular in the law enforcement sector and voice recognition is well suited for verification over phone lines. Now, let's take a closer look at Facial Recognition Technology**.**

fig1.



Face Recognition Biometrics

Face recognition technology involves analyzing certain facial characteristics storing them in a database and using them to identify users accessing systems. There are various recognition methods that emphasize identification based on the areas of the face that don't change, including:

- Upper sections of eye sockets
- Area surrounding cheek bones
- Sides of mouth

Face recognition technology works well with most of the shelf pc cameras, generally requiring 320 x 240 resolution at 3-5 frames per second. Obviously, better resolution cameras with higher frames per second will yield better quality images. You must combine the hardware with software. Facial recognition software products currently range in price from $59 to well over $1000, making it one of the cheaper biometric technologies.

The process flow is as follows:

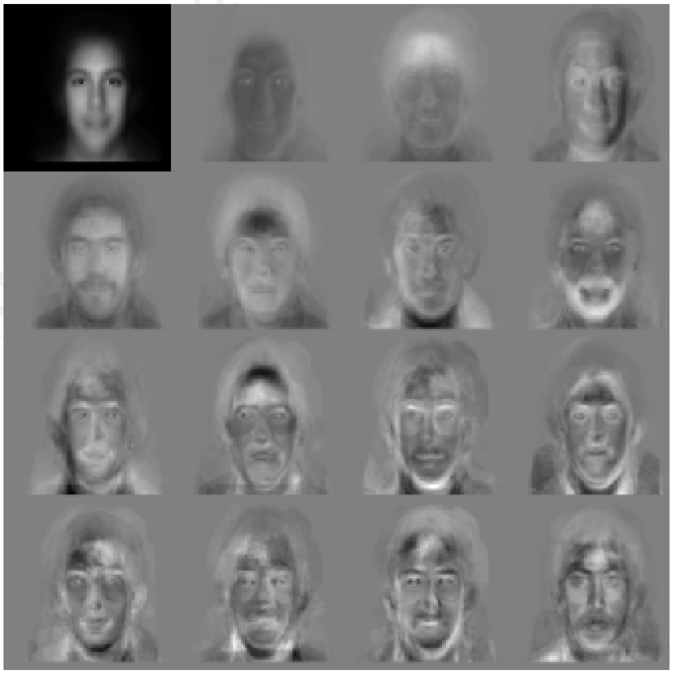
- Perform a sample capture
- Perform a feature extraction
- Perform a template comparison
- Perform matching

Authentication involves the user entering some identifying information, login name or pin, having a snapshot taken in front of the camera and then being verified or not.You may have seen facial recognition products currently implemented at airports and border crossings. It has the ability to track moving faces.

There are four primary methods used to identify and verify users. They include eigenfaces, feature analysis, neural network and automatic face processing.

Eigenfaces, which means roughly “one’s own face”, is a MIT patented technology which utilized two dimensional grayscale images representing distinctive characteristics of a facial image. (fig 2)

Fig 2



Feature Analysis is the most widely

used technology. It's claim to fame is that it is more capable of accommodating changes in appearance or facial aspect.

Neural Network analysis features from both faces, the enrollment and verification face and determine if there is a match using an algorithm

Automatic Facial Processing (AFP) uses distances and distance ratios between certain features of the face, namely eyes, end of nose and corner of mouth. Not as robust as eigenfaces, but would be more effective in dimly lit situation.

Conclusion

Although still a relatively new entry into the biometrics market, facial recognition is quickly emerging as a viable authentication method. With the adoption of standards and community awareness, this technology will become more mainstream. Current implementations of this technology are visible in airports, at ATM machines and border control checkpoints. Any good authentication system will not rely on only one technology but will include a combination of technologies.

References

Phillips, Ken. "Unforgettable Biometrics" PC Week Labs. 29 October 1997
URL: http://www.zdnet.com/eweek/reviews/1027/27bioapp.html (27 October 1997)

Evans, Mark. "Is Biometrics finally at hand?" ZDNet. 23 January 2001
URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2677548,00.html (23 January 2001)

Facial Scan.com. "How Facial Recognition Works"
URL: http://facial-scan.com/facial-scan_technology.htm

International Biometrics Group. IBG's Market Report
URL: http://www.biometricgroup.com/

Benado, Joe. "How it works: Biometric Security". 21 February 2001
URL: http://www.cnn.com/2001/TECH/ptech/02/21/biometric.works.idg/index.html

Woodward, John D. Jr. "And Now, the Good Side of Facial Profiling". The Washington Post . 4 February 2001
URL: http://washingtonpost.com/wp-dyn/articles/A23360-2001Feb3.html

Dam, Kenneth W. And Lin, Herbert S. "CRISIS: Cryptography's Role in Securing The Information Society. "NRC Project on National Cryptography Policy. 1996
URL: http://www.nap.edu/readingroom/books/crisis/frontmatter.txt 21 March 2000

Crume, Jeff "Inside Internet Security" Pearson Education Limited 2000