

Biometric Authentication, An Introduction

by: Keith Palmgren, 02/09/2005

<http://www.securitydocs.com/library/3003>

Historically, usernames and passwords are the most common form of authenticating computer users. They are also both the worst management headache for IT staff and the biggest network security hole in existence. Many help desks handle more password related calls than any other category. Users routinely share their passwords with one another. We have passwords on yellow sticky notes on the monitor and under the keyboard. If you don't find the password there, try the Rolodex® under "P" for Password.

Security industry observers frequently predict the use of biometric authentication systems will solve these problems. Those predictions are only beginning to come to fruition. Recent advances in technology coupled with a significant price drop make biometric authentication systems a viable alternative. As with most security solutions, proper implementation is critical. Deciding on the right type of biometric system requires an understanding of the underlying technologies.

Simply stated, biometrics are best defined as measurable human physiological and/or behavioral characteristics used to verify identity. In practice, biometric authentication systems typically combine a username or PIN with a fingerprint or other biometric identification mechanism. This leads to good security as it combines two authentication factors – "something you know" and "something you are". It is easy to share "something you know" such as a password with a coworker. Sharing "something you are" is much more difficult.

There is another significant advantage to biometrics. It is rare that security mechanisms have a positive impact on usability. Biometrics can indeed make a system easier to use since the user no longer has to remember passwords. This makes the user community happy and reduces calls to the help desk.

How Biometric Systems Work: While each biometric device and system has its own operating methodology, there are some general "rules of thumb" that you can expect to find in any system. The process for a given user will usually begin with an enrollment process. Here, the system captures one or more (typically three) samples of the biometric. These samples are stored in a "biometric template" and used for future comparison during authentication. Key elements in choosing a biometric system include ensuring that the enrollment process is relatively simple for the user, requires a short period of time, and provides for a high quality template.

After generation, the template needs to be stored. Since templates range from 9 bytes to around 1.5K in size, storage space is not typically a major issue except in very large implementations. There are typically three options for template storage.

- Store the template within the biometric reader itself. This provides for quick response during future authentication. However, it does not lend itself to situations where the user will need to authenticate at multiple locations. For example, a bank's ATM machines could not use this method since customers won't always use the same machine.
- Store the template remotely in a central repository. This overcomes the problem of users authenticating from multiple locations. There is the potential for "sniffing" the biometric data off the network and replaying the authentication session unless encryption is used. In addition, some users are very privacy conscious and do not like the idea of information such as fingerprint data being stored centrally.

- Store the template on a portable token such as a smart card. This method addresses the drawbacks of both previous methods. The biometric data is not centrally stored, does not traverse the network, and the user carries the information from location to location. Users also have a feeling that they control their personal identification data. The one drawback is that the cost of the biometric implementation is higher. You need a device to read the smart card as well as the biometric data.

Once enrollment and storage are complete, users authenticate themselves by matching the template against current input, usually referred to as “live data.” Most commonly, the user enters a username or PIN and then enters the live data (i.e. scans their fingerprint). Comparison of the live data and the template results in a simple binary yes/no match. “Verification” biometric systems tie the username or PIN to the template for a one-to-one match. While this is not the only method, it is the most common and reliable.

Types of biometric systems:

There are seven types of biometric measurements in common use today.

- ***Fingerprint Verification*** is perhaps the best-known type of biometric measurement. Fingerprint scanning products are the most common type on the market today. Properly implemented, fingerprints offer potential for high accuracy. In addition, the readers tend to be small (easily incorporated into a keyboard for example), have a relatively low cost, and integration is usually easy. Some potential problems can arise however. Cuts or dirt on the finger can cause some systems not to recognize a valid fingerprint. Some scanners require precise placement of the finger (others allow virtually any placement). Finally, give some thought to ensuring the finger is real and not some sort of copy. Some fingerprint scanners will scan for pulse as well as the fingerprint.
- ***Hand Geometry*** measure the physical characteristics of the user’s hand and fingers. Hand geometry is one of the most established methods and typically offers a good balance of performance and ease of use. Hand geometry is most widely used in physical access control and time/attendance systems. It is not currently in wide deployment for computer security applications primarily because it requires a large scanner.
- ***Voice Recognition*** is perhaps the method most desirable to users since everyone seems to want to talk to computers. In practice, implementation is extremely difficult. While recent advances in voice recognition have greatly improved the technology, it is still subject to problems. Local acoustics, background noise, microphone quality, the common cold, anxiety, being in a hurry, and anger can all alter the human voice enough to make voice recognition difficult or impossible. Further, voice recognition systems tend to have the most difficult and time-consuming enrollment process and require the most space for template storage.
- ***Retinal Scanning*** is well established and can provide high accuracy. User acceptance may be a problem however – “You’re not shooting a laser into my eye!” In reality, retinal scanners do not employ a laser, but scan using low intensity light and are considered quite safe. One drawback is that the user must look directly into the retinal reader. This is inconvenient for eyeglass wearers. In public applications, there may also be concerns with the spread of germs because of the need for physical contact with the retinal scanner. Another problem is that the user must focus on a given point for the scan. Failure to focus correctly causes a significant impact on accuracy.
- ***Iris Scanning*** overcomes most of the problems of retinal scanners. Because the iris (the colored part of the eye) is visible from a distance, direct contact with the scanner is not required nor is it necessary to remove eyeglasses. The technology works by scanning the unique random patterns of

the iris. Interestingly, the method does not rely on the iris color (the camera used is black-and-white). This is important because of the popularity of colored contact lenses – some vendors claim their systems will work with colored contacts and even through non-reflective sunglasses.

- **Signature Verification** enjoys a synergy the other technologies do not since people are used to signing for things. There is a greater feeling of normalcy. While signature verification has proved to be relatively accurate, very few products available implement the technology.
- **Facial Recognition** is one of the newest biometric methods. The technology has attracted a lot of attention. Unfortunately, extravagant claims that proved difficult to substantiate cooled much of the enthusiasm. It is not overly difficult to match two static images. Picking an individual out of a group as some systems claim to be able to do is another matter entirely. Progress continues to be made with this young technology, but to date facial recognition systems have had limited success in practical application.

Measuring Accuracy:

Accuracy of a biometric system is critical to successful implementation. Two measurements are commonly used. The likelihood that the system will incorrectly accept someone into the system is the False Accept Rates (FAR) or “False Positives.” How likely rejection of a valid user is falls under False Reject Rates (FRR) or “False Negatives.” Most biometric products allow administrators to adjust settings to lower the FRR number and make the system more user-friendly. However, there is typically a direct correlation between FAR and FRR. The lower the FRR percentage, the higher the FAR percentage and vice-versa. Finding a happy medium that keeps both False Positives and False Negatives to a minimum can be difficult. The degree of difficulty depends on the biometric method chosen and the vendor implementation.

Conclusion:

There is a good chance that biometric authentication will become more commonplace. While the technology exists for biometric use in E-commerce, the products will probably not become ubiquitous enough for that type of wide spread use in the near future. Enterprise implementations and specialized applications such as ATM machines are more likely.

Biometric Information Sources and Vendors – A to Z

[American Biometric Company](#)

Makers of the BioMouse, a desktop fingerprint authentication system.

[Association For Biometrics](#)

Non-profit organization aiming to promote the awareness of biometrics.

[Biometrics Consortium](#)

Extensive collection of information on research and development of biometrics.

[Biometrics Digest](#)

Online magazine covering news, vendors and general information on biometrics.

[Biometric Research](#)

A good overview from Michigan State University.

[Digital Persona's U.are.U](#)

Affordable, easy to use fingerprint identification for the home or office.

[Fight The Fingerprint](#)

An opposing point of view on biometrics.

[Human Identification in Information Systems](#)

An academic paper discussing the use of biometrics.

[PenOp](#)

PenOp is a leader in handwritten signature verification.

[Precise Biometrics](#)

Fingerprint identification vendor.

[SAFLink Corporation](#)

Products using voice, fingerprint or facial recognition.

Copyright <http://www.netip.com/>

NetIP, Inc. is a small company totally devoted to Knowledge Transfer. The President of the company, Keith Palmgren, divides his time between writing articles and teaching classes on Information Protection, Network Security, and Computer Security.