



## IT Security

### *The Basics of Biometrics for Computer Security*

*Author: Randy Bragg, MBA, MISM*

2613 Manhattan Beach Blvd Suite #100

Redondo Beach California 90278

Phone: 310.297.3605

Fax: 310.297.3615

Toll Free: 800.241.6808

## *The Basics of Biometrics for Computer Security*

Biometrics is a type of verification that can be used for authentication when using computers for a variety of purposes. In the past, the common perception of biometrics was that they were limited to use by government facilities and high security areas. However, biometrics are becoming more prevalent in day-to-day applications such as log-in access for laptop computers, access control to basic security doors, and a variety of other uses. Some of the more common uses are:

- 1) Time Clocks - Many time clocks are now designed for the potential use of biometrics for employee clock in and clock out. The most common types currently use a thumb print or fingerprint to verify the employee when clocking in/out.
- 2) Point-of-Sale Sign-in/out - Many point-of-sale systems are now integrating the use of biometrics for user sign-in and out. The thought behind this is that it eliminates the need for employees to either (1) carry a magnetic swipe card or (2) remember a password and punch it in every time.
- 3) Computer Log-in/out - Many computers (especially laptops) are now integrating some type of biometric control for the purpose of logging in and out. Most new laptops now have an index finger or thumb print scanner built in.
- 4) Alarm Activation/Deactivation - Biometrics are being integrated into many alarm panels for the purpose of activating or deactivating the alarm. When a person arrives or leaves a certain location, they could use a biometric scanner instead of a password to activate or deactivate the alarm.
- 5) General Access to Doors/Buildings/Etc. - Biometrics can be used for basic access control to any building, door, room, etc. Many types of locks and access control devices now use one or more biometric controls to allow access.

Just as there are many uses for biometrics, there are also several different types of biometric controls that may be used. They include:

1. Thumb or Fingerprint – Typically this involves the use of a thumb print or index finger print to authenticate the identity of the person. This is becoming very common on laptops and time clocks. For higher security applications, more than one fingerprint may be required. A drawback to this control is that fingerprints can change due to alterations in the skin, or fingerprints can be difficult to read due to oil, dirt, etc.
2. **Palm Geometry** – Palm Geometry involves the use of a person's palm print in order to identify a specific person. This type of control has the same drawbacks as the use of fingerprints.

3. **Hand Geometry** – Hand Geometry involves the use of a person’s entire hand including both the palm and fingers to provide authentication. This provides a higher level of security than either fingerprints or palm geometry, but has more potential for error due not being able to read the hand geometry or changes in a person’s hand.

4. Facial Recognition – Facial Recognition involves the use of a person’s facial features to identify a specific person. The drawback to this method is that a person’s facial profile can change over time.

5. Retinal Scanning – Retinal scanning involves the scanning of a person’s retina and then using the scan for identification purposes. The drawback to this method it that a person’s retina can change over time based on disease or astigmatism.

6. Iris Scanning – Much like DNA, iris scanning is one of the most reliable forms of identification. The drawback is that the technology is relatively new, expensive, and raises privacy concerns. However, this technology is expected to be extensively used in the future.

7. Speech Recognition – Speech recognition involves the use of a person’s speech pattern in order to verify his/her identification. This control is not widely used and is still primarily in the research phase as it has a high error rate.

8. DNA – This is by far one of the highest security controls that can be used for identification of an individual and it involves the matching of a person’s DNA profile for authentication. While very secure, the costs of this control are high and there are serious privacy issues.

As with many security devices, biometrics does not come without problems. Biometrics may be subject to two types of error. Biometric devices may (1) have false acceptance; that is allow someone into a certain location that should not have been granted access and (2) have false rejections; that is not allow someone into a certain location who should have been allowed in. While the normal security concern is to ensure the acceptance of only those who should be accepted, it is important to remember that too many false rejections can hamper productivity and access to the point that the device will be rejected by management.

One way to eliminate or reduce errors is the use of two factor authentication. In this method biometrics are combined with another type of authentication such as a personal identification number (PIN), password, or magnetic swipe card. For example, an employee may first swipe a magnetic card and then use a thumb print for added verification that someone else is not using their magnetic card. This procedure is typically used only for high security issues as it does add the extra burden of using two procedures. However, this procedure should not be overlooked even by the average business as it can provide excellent security for things such as safe access or access to security systems such as video surveillance systems.

Another area of concern with biometrics is privacy and security concerns. Just like with social security numbers, birth dates and personal information, the theft of biometric information can lead to identify theft. In addition, many individuals are rightfully concerned about organizations having access to their biometric information (as this is considered highly personal) and the potential for theft or accidental release of this information. The organization itself must also be extremely concerned with the security of this information. For example, if a hacker gains access to a thumb print database this would in turn allow them access to all user files if two factor

authentication is not used.

Biometrics can be used for many security-related functions such as time clock sign in/out, computer sign in/out, point-of-sale system access and general access control. While biometrics will be used more and more in the future, there are several issues that must be addressed including potential errors, privacy concerns and the security of the actual biometric images. Companies wishing to implement biometric controls would be advised to seek professional advice as this is a very complex field of security.