Biometrics – Basic Information

Biometric authentication involves using some part of your physical makeup to authenticate you. This could be a fingerprint, an iris scan, a retina scan, or some other physical characteristic. A single characteristic or multiple characteristics could be used. It all depends on the infrastructure and the level of security desired. With biometric authentication, the physical characteristic being examined is usually mapped to a username. This username is used to make decisions after the person has been authenticated. In some cases, the user must enter the username when attempting to authenticate; in others, a lookup is done on the biometric sample in order to determine the username.

Biometric authentication is performed by doing a comparison of the physical aspect you present for authentication against a copy that has been stored. For example, you would place your finger on a fingerprint reader for comparison against the stored sample. If your fingerprint matches the stored sample, then the authentication is considered to be successful.

In order to set up biometric authentication the appropriate infrastructure must be in place. Once the infrastructure is set up we register users. Some products allow users to register directly while others require a registration agent to perform the registration for the user. Let's take the example of fingerprint-based authentication.

During the registration process, the system will ask the user to submit a sample, in actual fact it will create multiple samples. The user places their finger on the fingerprint reader. The system will record images of the user's fingerprint. The system will use the multiple images to determine a point pattern to identify the user's fingerprint. These points are basically dots placed on different areas of the fingerprint. These dots are used to denote the pattern made by the fingerprint. Once a sufficient number of samples have been taken to form a consistent point pattern, the pattern is stored and used as the basis for later comparison during authentication.

Thanks to: siencedirect.com
Data source