12. Strengths and Weaknesses of Biometrics

Elaine M. Newton[18]

Introduction

In general, there are three approaches to authenticating an individual's identity. In order of most secure and convenient to least secure and convenient, they are as follows:

Something you are: a biometric such as a fingerprint.

Something you know: a PIN, such as an ATM bank account password.

Something you have: key, token, card, such as an ID card.

Any combination of these approaches can potentially further heighten security.

Facial recognition software, fingerprint readers, hand geometry readers, and other forms of biometrics appear increasingly in systems with mission-critical security. Given the widespread consensus in the security community that passwords and magnetic-stripe cards accompanied by PINs have weaknesses, biometrics could well be ensconced in future security systems.

This document begins with a definition of biometrics and related terms. It then describes the steps in the biometric authentication process, and reviews issues of template management and storage. The appendix concludes with a brief review of mainstream biometric applications.

---

18 as adapted from John D. Woodward, Katherine W. Webb, Elaine M. Newton et al., Appendix A, "Biometrics: A Technical Primer," "Army Biometric Applications: Identifying and Addressing Sociocultural Concerns," RAND/MR-1237-A, Santa Monica, CA: RAND 2001.

Overview

A biometric is any *measurable*, *robust*, *distinctive* physical characteristic or personal trait that can be used to identify, or verify the claimed identity of, an individual. Biometric authentication, in the context of this report, refers to automated methods of identifying, or verifying the identity of, a living person.

The italicized terms above require explanation.

Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format. This allows for the automated matching process to occur in a matter of seconds.

The robustness of a biometric is a measure of the extent to which the characteristic or trait is subject to significant changes over time. These changes can occur as a result of age, injury, illness, occupational use, or chemical exposure. A highly robust biometric does not change significantly over time. A less robust biometric does change over time. For example, the iris, which changes very little over a person's lifetime, is more robust than a voice.

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The higher the degree of distinctiveness is, the more unique the identifier. The highest degree of distinctiveness implies a unique identifier. A low degree of distinctiveness indicates a biometric pattern found frequently in the general population. The iris and the retina have higher degrees of distinctiveness than hand or finger geometry.

The application helps determine the degree of robustness and distinctiveness required. The system's ability to match a sample to a template is sometimes referred to as the biometric's reliability.

Systems can be used either to identify people in a consensual or non-consensual manner - as when faces are scanned in public places - or to verify the claimed identity of a person who presents a biometrics sample in order to gain access or authorization for an activity. The following section expands on this issue.

"Living person" distinguishes biometric authentication from forensics, which does not involve real-time identification of a living individual.

Identification and Verification

Identification and verification differ significantly. With identification, the biometric system asks and attempts to answer the question, "Who is X?" In an identification application, the biometric device reads a sample and compares that sample against every template in the database. This is called a "one-to-many" search (1:N). The device will both make a match and subsequently identify the person or it will not make a match and not be able to identify the person.