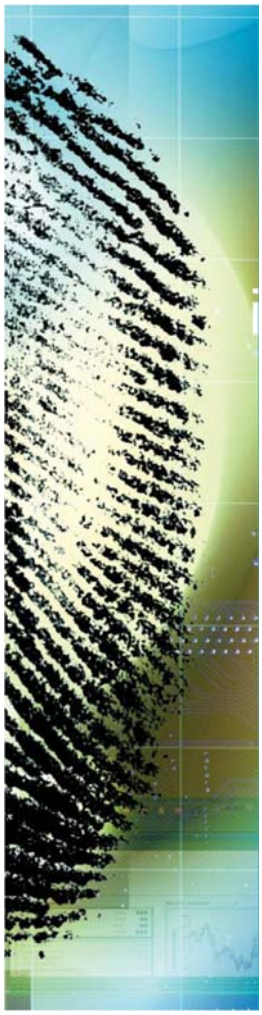
Systems and Network Analysis Center
Information Assurance Directorate

Biometrics Security Considerations



What is Biometrics?

A biometric characteristic is a general term used to describe a measurable physiological and/or behavioral characteristic that can be used for automated recognition. A biometric system provides an automated method of recognizing an individual based on the individual's biometric characteristics. Biometric modalities commonly implemented or studied include fingerprint, face, iris, voice, signature, vein pattern, and hand geometry. Many other modalities are in various stages of development and assessment.

Biometric systems are commonly used to control access to physical assets (laboratories, buildings, cash from ATMs, etc.) or logical information (personal computer accounts, secure electronic documents, etc). Biometric systems can also be used to determine whether or not a person is already in a database, such as for social service or national ID applications.

The operation of a biometric system can be described, in a simplified manner, by a three-step process. The first step in this process involves an observation, or collection, of the biometric data. This step uses various sensors, which vary between modality, to facilitate the observation. The second step converts and describes the observed data using a digital representation called a template. This step varies between modalities and also between vendors. In the third step, the newly acquired template is compared with one or more previously generated templates stored in a database. The result of this comparison is a “match” or a “non-match” and is used for actions such as permitting access, sounding an alarm, etc.

Declaring a match or non-match is based on the acquired template being similar, but not identical, to the stored template. A threshold determines the degree of similarity required to result in a match declaration. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Some biometric systems employ liveness detection. Liveness detection is used to ensure that only characteristics from a living human being can be used in a biometric system and enables the detection of spoof attacks (e.g., submission of a fake biometric sample.)

3-Factor Authentication

What you have:
- **Token**

What you know:
- **Password or PIN**

What you are:
- **Biometrics**

Biometrics Considerations

While potentially offering significant security benefits, a biometric system is only one of many security tools available. Depending on the application, an environment or circumstance may or may not benefit from a biometric system. Understanding the operational requirements of the situation is necessary to determine if a biometric system can be used to meet a security need. The use of biometrics will not solve all of a system’s security problems, but when properly implemented, a biometric system should be one part of an overall security architecture.

There is no single biometric modality that is best for all applications. Many factors must be taken into account when implementing a biometric system including location, security risks, task, expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity and therefore may offer varying levels of security, ease of implementation, and user convenience.

SNAC DoD, 9800 Savage Rd Ft. Meade, MD 20755-6704 410-854-6632 DSN 244-6632 FAX: 410-854-6604 www.nsa.gov/snac

Biometric systems alone do not currently provide adequate security for high assurance applications. When biometric systems (something you are) are combined with other security mechanisms (something you have and something you know), those systems can provide significant security benefits. However, the biometric system must be implemented correctly for the specific application.

False Accept Rates

Most biometric systems will advertise a False Accept Rate (FAR) and False Reject Rate (FRR) to characterize the security provided by the system. The FAR tells you how often someone will be recognized successfully when he/she should not have been recognized, and the FRR tells you how often someone who should have been recognized successfully is not recognized. When addressing the security of the biometric system, these numbers can be misleading, especially the FAR.

Most biometric systems claim FARs in the 1 in 10,000 to 1 in 1,000,000 ranges. As a loose comparison, 128-bit AES has an approximate cryptographic strength of 1 in 10^{38}. Yet, the FAR is an upper bound on security, so the actual strength of mechanism is a much harder characteristic to ascertain and is likely to be much lower.

The FAR assumes random and real samples of the biometric characteristic are presented to the system. Attackers don't have to use random or real samples; they are much more likely to pick samples intelligently and achieve a much higher FAR. The attacker can do this in two ways. First the attacker can use a copy of the biometric characteristic of a valid user collected by the system to produce a fake biometric characteristic that will allow access. This attack is called a physical spoof attack and will allow the attacker to bypass the biometric system. This attack is loosely comparable to an attacker finding a password written down or watching a valid user enter a password, copying it, and using it to gain access to the system. Second, if the attacker does not have a copy of the biometric characteristic of a valid user, the attacker can attempt to create a fake biometric characteristic by guessing "intelligently" or the attacker can use a database of real samples of non-valid users "intelligently" instead of randomly. As the guesses get better, the attacker will likely bypass the biometric system in fewer attempts than presenting random samples. This is loosely comparable to an attacker using a dictionary to attack a password-based system rather than randomly going through all possible passwords of the proper lengths. Dictionaries allow the attack to succeed much more rapidly than random guessing. For biometric systems, liveness detection makes both attacks more difficult. However, while liveness detection is improving in biometric systems overall, many systems employing liveness detection are still susceptible to physical spoof attacks.

Rather than attacking using samples of the biometric characteristic, other attacks on a biometric system may be possible, such as cryptographic attacks, network attacks, operating system attacks, etc. All these potential vulnerabilities must be considered when implementing a biometric system with the intent of enhancing system security.

Biometrics at IAD

With respect to biometrics, the Systems and Network Analysis Center's mission is to provide customers with vulnerability evaluations of biometric authentication systems. We discover vulnerabilities, recommend countermeasures to mitigate the discovered vulnerabilities, and provide implementation guidance.

There are several types of biometric systems to choose from when implementing an access control system. Which one(s) we recommend depends on your specific requirements. For physical access control applications, we almost always recommend using the biometric system in conjunction with other security mechanisms, such as card readers, PINs, and/or an attentive guard. For logical access control, biometric systems can provide some added security, but these also should be used in conjunction with other security mechanisms, such as passwords and/or tokens. We do not recommend using a biometric system in place of a password or other established security mechanism for logical access, but only as an added layer of security.