Explainer: Verification vs. Identification Systems

Biometrics are typically applied to identify a person or verify a claimed identity. Identification and verification are different processes that play similar roles in different kinds of security systems. Though the two concepts overlap and are sometimes used interchangeably in public discourse, there are critical distinctions that must be noted.

Identification is the task of answering: “Who is this person?” It consists of receiving data about an unknown individual, such as a photo of their face, their voice biometrics or fingerprints, and comparing it to a larger database to uncover a potential match. Identification systems are described as a 1-to-n matching system (sometime written ‘1:N’), where n is the total number of biometrics in the database. Identification tends to take longer than verification, as the algorithm must compare the reference data against a larger set of subjects to find a match.

Forensics labs are one example of an identification operation, as they store large banks of biometric data ranging from fingerprints and DNA samples collected at a crime scene. That information is then compared to newly-provided samples to prove the presence of the suspect.

Verification asks “Is the person who they say they are?” A person identifies as a certain user, and must provide proof they can confirm their identity compared to already-stored data. Verification is a 1-to-1 (or ‘1:1’) matching system because it aims to match a specific individual, rather than cast a wide net to find similarities in the identification process. Also, verification usually works more rapidly than identification, as it filters for highly-specific parameters in a smaller database.

Authentication is another concept in biometric matching, closely aligned with verification. A similar process to that used in identity verification is applied to subsequent interactions to authenticate that the person is the same one whose identity has previously been verified.

Consumer technologies such as smartphones employ verification to unlock their use, often with the application of fingerprint scanners or facial recognition systems.

.

Comparison of the 1:1 and 1:N authentication methods

In biometry, there are two methods for identifying people, based on the pool of templates the identification is performed on. These are the 1:1 method, or verification and the 1:N method, or identification. Both has its own pros, cons and suggested usages, and this blogpost is aimed at providing a basic understanding of the two concepts along with their properties.

Identification (1:N method)

In this case, every person enrolled in the system is stored in the same database. The term identification stems from the fact that the system, when presented with a user sample, will search through the whole database in order to establish the identity of the person, by choosing the template most similar to the sample in question. This system alone is a single factor authentication, as nothing else beyond the biometric sample is required to identify the person.

Pros

- The system stores templates in a central database, thus it is cheaper to maintain than a 1:1 system that stores the templates individually on external devices
- The system can provide higher throughput rates than a 1:1 system, for authentication requires only one step, ideal for places where mass acceptance is a factor (e.g. stadiums)
- The stored template is harder to tamper with, as access to the database is usually properly limited

Cons

- Privacy concerns may arise as templates are owned by the system operator rather than the owners of the samples
- User numbers may have an impact on the performance, as the system must match each sample to every template within the database
- Higher FAR rates may apply as there are many templates in the database, that may be similar

Verification (1:1 method)

In this case, people may or may not be stored in a central database. If it is stored in a database, when performing verification, it is pre-selected by some other method (e.g. PIN, RFID card, or another biometric factor), thus being a multi-factor authentication method in itself, and after the pre-selection, the presented sample is only matched against that template. The sample could be also stored on an external device (e.g. an RFID smartcard), and the system will only check if the presented sample is identical to the stored template.

Pros

- It is possible to let users own their templates on a possession based device, eliminating privacy concerns
- User number does not affect performance, as the system always have to match the sample to only one template
- Being a multi-factor authentication in itself, this method can allow for higher security levels, if implemented properly

Cons

- If RFID cards are used (especially if smartcards that allow for template storage), the system can be significantly more expensive
- If the template is owned by the user (and it is either a user of malicious intents or the device is stolen), a rather large time frame is available for an attacker to tamper with the template
- The system has lower throughput as authentication requires two or more steps, that take time

Summary

As we can see, neither method is absolutely better or worse than the other, and neither has a clearly cut area where it should be used exclusively. Each potential installation location should be assessed carefully in order to determine which method is the more practical and what standpoints are there to consider. Many devices nowadays can provide both 1:1 and 1:N methods for use, even within the same system, which means that it is possible to have an access point perform identification and a different one to perform verification. An example for this could be a main entrance, where only biometry has to be used in the 1:N method for better throughput, while restricted areas may require a PIN code or an RFID card or another biometric feature in order to perform 1:1 verification. The options are vast in number, and as such, they should be weighed carefully during a planning phase.