

7.4 Biometrics Design Alternatives

This pattern aids the selection of appropriate biometric mechanisms to satisfy I&A requirements. Biometric mechanisms considered are face recognition, finger image, hand geometry, iris recognition, retinal scanning, signature verification, and speaker verification. Additional mechanisms, including DNA, are identified for completeness.

Example

The internal maintenance and research areas of the new gemstone wing of the museum essentially afford staff access directly to high-value assets and to the information on those assets. While physical entry for these activities is being tightly controlled, access to sensitive asset information must also be restricted. To gain access to the Web server with strictly controlled asset information, staff are required to log-on to the Web server. Part of the log-on process will be use of a biometric to provide additional verification of employee identities. Alvin the system architect must determine which biometric mechanism is most appropriate for the museum.

Context

The person applying this pattern understands the requirements for I&A, along with their relative importance, for example from the results of applying I&A REQUIREMENTS (192).

A decision has been made to use biometrics for I&A, for example from the results of applying AUTOMATED I&A DESIGN ALTERNATIVES (207), but which biometrics technique to use has not been decided. The decision to use some form of biometrics is typically made in the context of a user population of limited size, because of the enrolment effort required.

Discussion: What do all biometric mechanisms have in common?

All biometric mechanisms share an underlying methodology involving enrolment (which is outside the scope of this pattern) and verification or identification. At enrolment, the person offers a 'live sample' of the biometric, such as a finger image. This is scanned electronically, processed and stored as a template, which is a mathematical representation of the original sample. Once the template is captured, the original sample data is no longer used and is discarded. Alternatively, it might be wise to keep the original raw sample data, against the possibility that better template-algorithms and representations might become available in the future: in some areas such

as fingerprint recognition, technology is changing and significant improvement can be expected. Keeping the raw sample data would allow one to benefit from newer algorithms without the need to re-enrol all users.

To confirm identity at a future time, the individual presents the live sample, which is matched against the stored template. In a 1:many search, the individual presents only the live sample, and the database is searched for a match. This is called *identification*. In a 1:1 search, the user presents a name or other identifier along with the live sample. The system checks the live sample only against templates stored under that identifier. This is called *verification*. [Seffers2001].

When biometrics are used for verification, the captured biometric record is matched against one biometric template in the data store to determine a match. The one biometric template in the data store is found by association with a presented identifier, acquired separately via non-biometric means such as a token. This is a 1:1 match, and answers the question 'Am I who I say I am'?

When biometrics are used for identification, the biometric capture and conversion are the same, but no separate identifier is acquired, and therefore the verifier matches the biometric record against all biometric records in the data store. If a match is found, the associated identifier is found. This is a 1:many match, and answers the question 'Who am I'? The result is still success or failure, and in the case of success, an identifier is produced. If the identifier is considered to be verified or authenticated, then in effect the biometric technique provides a full I&A solution.

Problem

Each technique has different strengths and weaknesses, which are described in the Implementation section. Therefore, no one technique or combination of techniques is best for all enterprises. Decisions are needed to determine the best biometric mechanisms for the given purpose.

It should be noted that biometrics, at least in human-readable form, have been available for a long time, even before the term 'biometrics' was used. For example, badges, licenses, and passports have often included photographs as well as physical characteristics such as height and eye color. Fingerprints have long been used in criminal justice and other security contexts.

Given that biometrics has been selected to perform some I&A purpose, what biometric mechanisms would best satisfy this purpose?

Selection of appropriate biometrics mechanisms needs to resolve the following forces:

Biometrics have Vulnerabilities and Limitations

- Some biometric information can be stolen, for example, by obtaining and using pictures, images, imprints, or other models of another person's biometric information.

- Biometric information can be erroneously associated with the wrong identity at enrollment: for example, actor B can enrol his biometric information with actor A's identity.
- Stolen or erroneously enrolled biometric information can be used to masquerade as another person, which leads to false acceptance.
- Some biometric measurements can vary due to environmental conditions, or can change over time due to age, or can change quickly due to injury, surgery, or other significant episode. Such variations can lead to false rejection.

Biometrics have Two Conflicting Error Types

- False acceptance can lead to unauthorized access to assets, in cases in which an access control service relies on the biometric mechanism's results.
- False acceptance can lead to lack of accountability, in cases in which an accounting service such as audit relies on biometric mechanism results. If actor B successfully masquerades as actor A, then actor A is erroneously held accountable for the actions of actor B.
- False rejection can lead to reduced productivity and increased user frustration.
- False rejection can also lead to lack of accountability. For example, actor A may take steps to change certain biometric characteristics via surgery with the goal of being falsely rejected as actor A. This may allow him to avoid accountability for an action such as a serious crime.
- In general, low false acceptance rate (FAR) and low false rejection rate (FRR) are conflicting goals: configuring a biometric mechanism to achieve a very low FAR tends to increase the FRR. Conversely, achieving a very low FRR tends to increase the FAR. When comparing biometric systems, a low FAR is most important when security is the priority. On the other hand, a low FRR is most important when convenience is the priority. [Liu2001] discusses the inverse relation between these two error types.

Biometrics have Other Forces to Consider

- Some biometric mechanisms cost more than others.
- Some biometric mechanisms require more equipment and changes to the infrastructure than others.
- Some biometric mechanisms are less safe than others.
- Enterprise-wide optimization affects selection of biometric techniques. An enterprise may find it more efficient—for example, for cost, training, and maintenance reasons—if all I&A domains that select biometrics use the same biometrics technique. For example, an enterprise may decide that the biometrics used in granting physical access to all enterprise facilities throughout the country should use the

same technique. Therefore, the selection of specific mechanisms may be a significant decision.

Solution

Systematically review the characteristics of available biometric mechanisms or techniques, and select a mechanism. Several well-known biometrics mechanisms exist. Different mechanisms have different strengths and weaknesses and emphasize different characteristics. Each technique resolves each force to a different degree than the others. The solution provides information about alternative biometric mechanisms that is intended to help differentiate them and to help select the best technique for a given purpose, enterprise, and I&A use.

All biometric techniques can be used for verification, but only a few are capable of performing identification, especially in a large population of users or actors. This is because the task of matching a live sample with one designated template is much simpler than finding a template from a large number of possible templates. According to [Ashbourn2000], the only biometric mechanisms with the capability to operate realistically in identification mode are finger image, iris recognition, retinal scan, and, to a lesser degree, facial scan.

Structure

Table 7.5 shows elements of the structure of this solution. Required capabilities and properties in the first column are derived from the general I&A REQUIREMENTS (192) pattern. Specialized selection criteria in the second column are additional factors related specifically to biometric mechanisms. Together, requirements and specialized criteria drive the selection of biometric mechanisms listed in the third column. Specialized criteria are further explained in the Implementation section.

Dynamics

This section describes the steps in the process of applying the pattern. Biometrics I&A inputs, including domain definition and requirements, are assembled first. Next, the specific characteristics of each biometric technique are defined, followed by selecting the best individual technique. If this technique is to be used as a stand-alone I&A mechanism, the process is then complete. If the technique is to be combined with another I&A technique—typically a non-biometrics technique, the combined strategy defined, for example, by AUTOMATED I&A DESIGN ALTERNATIVES (207)—then the selected biometric technique must be integrated with the other technique to form an integrated I&A solution.

Table 7.5 Elements of biometrics design solution structure

REQUIRED CAPABILITIES/ PROPERTIES	SPECIALIZED SELECTION CRITERIA	BIOMETRIC MECHANISMS
<ul style="list-style-type: none"> • Avoid false positives • Avoid false negatives • Variety of user types • Variety of user locations • Variety of user mobility • Easy to use • Speed to use • Safety of use • Cost effective • Compatible with infrastructure • Able to protect authenticators • Provide availability of process 	<ul style="list-style-type: none"> • Devices needed • Obtrusiveness • Accuracy • Resistance to attack (secure) • Public acceptance • Biometric long-term stability • Potential interference • Template size 	<ul style="list-style-type: none"> • Face recognition • Finger image • Hand geometry • Iris recognition • Retinal scanning • Signature verification • Speaker verification

Implementation

The description and characteristics of biometric mechanisms provided here is intended to help select appropriate biometrics for a specific context. Differentiating factors include degree of accuracy, ease of use, processing speed, and size of template—the amount of data to be captured and processed. The set of biometrics, and definition of each, are obtained primarily from [AFB1999].

Each technique is classified as being based on either a physical or a behavioral characteristic. In the set identified here, the behavioral biometrics are signature verification and speaker verification, although the latter is part behavioral and part physical. The remaining biometric techniques are classified as physical.

Additional biometric techniques that exist include:

- DNA, which carries the unique genetic instructions for an individual
- Keystroke dynamics, the typing rhythm when a user types onto a keyboard, ear shape, the outer ear, lobes, bone structure
- Finger geometry, the shape and dimensions of one or more fingers
- Palm geometry, the shape of the lines on the palm of the hand
- Veincheck/Vein tree, which uses pattern of veins in the back of the hand

We do not consider these techniques further in this pattern because they are not yet commonly used for I&A. Keystroke dynamics shows promise, but has not yet reached a high level of accuracy.

234 Chapter 7 Identification and Authentication (I&A)

Characteristics of the more common biometric mechanisms are summarized in Table 7.6. The value indicates the extent to which a technique satisfies a requirement for a particular factor. ‘High’ indicates high satisfaction of the factor, ‘Low’ indicates low satisfaction, and so on.

The potential interference factor identifies conditions that can inhibit successful operation of the mechanism. In general, one has to consider the basic characteristic of the concrete implementation of the technique. For example, background noise can interfere with voice recognition, or poor lighting can interfere with face recognition.

Table 7.6 Characteristics of common biometrics techniques. Reproduced by permission of ICSA Labs

TECHNIQUE FACTOR	FACE	FINGER	HAND	IRIS	RETINA	SIGNATURE	VOICE
Accuracy	High	High	Med/high	Very high	Very high	Medium	Medium
Ease of use	Medium	High	High	Medium	Low	High	High
Resistant to attack, secure	Medium	High	High	Very high	Very high	Medium	Medium
Public acceptance	Medium/ High	Medium	High	Medium	Medium	Very high	High
Long-term stability	Medium	High	Medium	High	High	Medium	Medium
Potential interference	Lighting, aging, glasses, hair	Dryness, dirt, age, race	Hand injury, age	Poor lighting	Glasses	Changing signatures	Noise, colds, weather
Safety	High	High	High	High	Medium	High	High

To determine the biometric mechanism that will best satisfy the biometric’s purpose, you can compare the technique profiles with your results of applying I&A REQUIREMENTS (192) to find a mechanism that is most compatible with your specific requirements.

Characteristics of Each Biometric Mechanism

The more common techniques are now described in more detail, especially the features and considerations that affect their selection. The details are obtained primarily from [Tilton2002].

Table 7.7 describes the characteristics of face recognition, which is a physical biometric technique that analyzes distinguishing facial features.

Table 7.7 Face recognition. Reproduced by permission of the SAFLINK Corporation

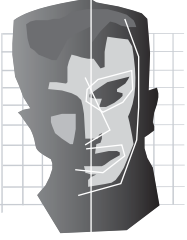
CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 <p>Still camera, video, thermal imaging</p>	<ul style="list-style-type: none"> • Can use standard video camera input • Can be used passively (unobtrusively) and with existing photo databases • Socially acceptable • Compatible with existing ID systems such as drivers license, passport 	<ul style="list-style-type: none"> • Can be affected by lighting and sometimes by skin tone, eyeglasses, facial hair, or expression • Twins harder to distinguish • Changes over time may require update/adaptation • Occasional religious objections and recent privacy objections to covert use • 600–3500 byte template size

Table 7.8 describes the characteristics of finger image, which is a physical biometric technique that looks at the patterns found on the tip of the finger. Finger images may be captured by placing a finger on a scanner, or by electronically scanning inked impressions on paper. It is one of the oldest biometric approaches.

Table 7.8 Finger image. Reproduced by permission of the SAFLINK Corporation


CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 <p>Usually a small reader (sensor) embedded within a stand-alone device or a peripheral, such as a keyboard, PCMCIA card or mouse.</p> <p>Sensor types include optical, silicon chip, ultrasonic</p>	<ul style="list-style-type: none"> • Significant proven use since largely easy to use and very quick • Relatively high accuracy • Variety of applications and products from numerous vendors 	<ul style="list-style-type: none"> • Requires dedicated device • A small percentage of population have poor images due to injury, disease, or occupation • Dry skin can reduce accuracy • Some lingering criminal connotations • Overt action generally required, somewhat obtrusive • 250 B–1 Kbytes template size

Table 7.9 describes the characteristics of hand geometry, which is a physical biometric technique that involves analyzing and measuring the shape of the hand from a 3-D perspective. This is one of the oldest biometric approaches.

Table 7.9 Hand geometry. Reproduced by permission of the SAFLINK Corporation

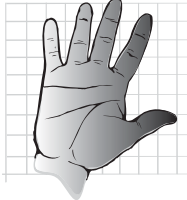
CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 Hand reader, including camera	<ul style="list-style-type: none">• Ease of use, fast capture and processing• Very small template size (~9 bytes)• Outdoor environments	<ul style="list-style-type: none">• Requires bulky device• Only moderate differentiation and accuracy• Used mostly for verification, not identification

Table 7.10 describes the characteristics of iris recognition. This is a physical biometric technique that analyses iris features found in the colored ring of tissue that surrounds the pupils.

Table 7.10 Iris recognition. Reproduced by permission of the SAFLINK Corporation

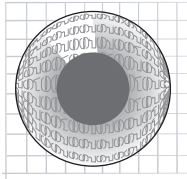
CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 Cameras, standard video technology	<ul style="list-style-type: none">• Highly accurate, highly differentiating (each eye averages 266 unique features)• Can support identification as well as verification• Very stable over lifetime• Passive collection (non-obtrusive)• Not affected by common eye surgical procedures	<ul style="list-style-type: none">• Requires dedicated device (some dual-use devices are available)• Mirrored sunglasses can interfere• Affected by some eye diseases such as cataracts• Limited focal length (4" to 3'), depending on device• 500 byte template size

Table 7.11 describes the characteristics of retinal scanning. This is a physical biometric technique that analyses the layer of blood vessels situated at the back of the eye.

Table 7.11 Retinal scanning. Reproduced by permission of the SAFLINK Corporation

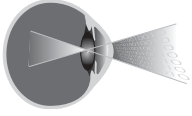
CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 <p>Low intensity light source (laser) with optical coupler</p>	<ul style="list-style-type: none"> • High accuracy and stability, difficult to falsify • Minimal alignment and focus problems • Can support identification as well as verification 	<ul style="list-style-type: none"> • User interface generally considered intrusive and uncomfortable • Safety concerns, possible damage if laser intensity too high • Capture can take several seconds • Devices still somewhat expensive • 96 byte template size

Table 7.12 describes the characteristics of signature verification. This is a behavioral biometric technique that analyses the way someone signs their name. The signing features such as speed, velocity and pressure exerted by the hand are as important as the static shape of the finished signature.

Table 7.12 Signature verification. Reproduced by permission of the SAFLINK Corporation

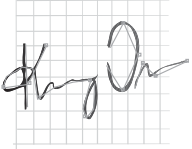

CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 <p>Signature or graphics tablets, special pens</p>	<ul style="list-style-type: none"> • Non-intrusive, natural act, highly acceptable • Particularly compatible with financial or legal transactions, orders, document signing • Many can already use built-in graphics devices, such as those in PDAs • Can work with Arabic lettering or Asian characters 	<ul style="list-style-type: none"> • Requires multiple consistent captures for enrolment • Can be affected by behavioral factors such as stress, distractions • May change over time, require update/adaptation • Best used in 1:1 contexts, that is, verification, not identification • 1–3 Kbyte template size

Table 7.13 describes the characteristics of speaker verification. This is a part physical, part behavioral biometric that analyses patterns in speech. It compares live speech with a previously-created speech model of a person's voice.

Table 7.13 Speaker verification. Reproduced by permission of the SAFLINK Corporation

CAPTURE DEVICES	FEATURES (+)	CONSIDERATIONS (-)
 Audio capture devices (sound cards, microphones)	<ul style="list-style-type: none">• Socially acceptable and non-intrusive• Can use standard handset, sound cards, microphones, over existing audio channels such as telephone lines• Can be combined with challenge/response mechanisms• Algorithms are typically language independent• Generally cannot be defeated by tape recordings or mimics	<ul style="list-style-type: none">• Can be affected by illness, stress, or background noise• Can be susceptible to high-quality digital audio playback attack• Requires similar microphones for enrolment and verification• May change over time, require update/adaptation• Best used in 1:1 contexts, that is, authentication, not identification• 6 Kbyte template size

Combining Mechanisms

If the purpose of the selected biometric mechanism is to perform verification, then the mechanism may need to be combined with a non-biometric I&A technique for a full I&A solution. The recommendation in this case is to apply AUTOMATED I&A DESIGN ALTERNATIVES (207) if you have made a decision to use only automated I&A, either prior to, concurrent with, or subsequent to, the application of BIOMETRICS DESIGN ALTERNATIVES (229).

Selecting a Biometric Mechanism

While the scope of this pattern is the selection of a biometric mechanism for one I&A use, this decision does not occur in a vacuum. Decisions made on biometric mechanisms for other similar I&A uses within the enterprise may influence the decision for a given biometric approach. In addition, more than one biometric may be needed and consideration will need to be given to the interaction of those mechanisms.

Example Resolved

Alvin the system architect determines that for the museum, part of the log-on process will use a biometric to provide additional verification of employee identities. The museum wants at least high confidence with regard to the accuracy, ease of use, and resistance to attack of the biometric selected. Only the iris scanning and

Table 7.14 Museum resolution for biometrics

TECHNIQUE FACTOR	IRIS	FINGER
Accuracy	Very high	High
Easy to use	Medium	High
Resists attack (secure)	Very high	High
Public accepts	Medium	Medium
Long-term stability	High	High
Potential interference	Poor lighting	Dryness, dirt, age, race
Safety	Medium	High

fingerprint approaches can provide high confidence for those important criteria, as shown in Table 7.14.

To address the concerns of their staff, Alvin chooses fingerprint detection as the preferred biometric mechanism, as the technology is known to be safe and easy to use, and the potential interference factors are not expected to be extreme for this environment.

Known Uses

Use of biometrics techniques is increasing, but the decision process for deciding among biometrics alternatives is generally tacit and informal, as opposed to being codified or published. However, discussion of the characteristics of various biometrics techniques does exist. [Smith2002] describes common characteristics and processes for biometrics I&A, as well as security of biometrics information. [Tilton2002] and [Liu2001] provide more details of variations among biometrics techniques, and are the sources of much of the implementation information in this pattern.

Consequences

The following benefits may be expected from applying this pattern:

- It fosters engineer awareness of the elements of the decisions needed for selecting biometrics techniques.
- It facilitates conscious and informed decision making about biometrics to support identified identification and authentication service needs.

- It encourages better balance among competing biometrics selection forces and factors, including the inherent trade-off between the rates of false acceptance and false rejection, as well as theft, environmental impact, cost, and infrastructure impact. The result is increased likelihood that a biometrics technique will be selected that satisfies the most important requirements.
- It provides some assistance about how you can combine biometrics with other mechanisms to provide a complete I&A service.
- It facilitates broader enterprise optimization by promoting integration of biometrics choices across multiple domains and systems across the enterprise.

The following potential liabilities may result from applying this pattern:

- It requires an investment of resources to apply the pattern, including time to analyze biometrics mechanisms.
- Perception of identification and authentication (I&A) needs can differ throughout an organization. This may make it difficult to reach agreement on priorities for I&A, and therefore difficult to select a biometric mechanism. On the other hand, bringing such disagreements to the surface may be a benefit, because then they can be properly discussed and resolved.
- Although biometric techniques work well today for authentication with a given ID, the techniques are less reliable for identification from a large user base. This point is often neglected by decision makers.
- Users and organizations may have a false sense of increased security, because they are using technology that is more expensive and more sophisticated. The cautions of this pattern over theft and other limitations of biometrics may not overcome the general perception promoted in some of the literature that biometrics is infallible.
- The enrolment process for biometrics can be expensive, because its users need to provide samples in a protected environment, otherwise an imposter might be able to submit their sample under a false identity.
- If the biometrics sensor and the storage of the templates or the checking mechanism are coupled by a network, an intruder can either steal valid samples or templates for later misuse, or can perform a denial of service attack.

See Also

After applying this solution, the next step typically is to apply the selected technique, which might be any of these:

- FACE RECOGNITION (65)
- FINGER IMAGE (65)

- HAND GEOMETRY (65)
- IRIS RECOGNITION (65)
- RETINAL SCANNING (65)
- SIGNATURE VERIFICATION (65)
- SPEAKER VERIFICATION (66)

Each of these is a potential pattern, but none is included in this book. Thumbnails of these patterns can be found in Chapter 5, *The Security Pattern Landscape*.