

A Biometric Standard for Information Management and Security

Stephen M. Matyas Jr.¹ and Jeff Stapleton²

¹IBM Corporation, Research Triangle Park, NC 27709, USA.

²KPMG Peat Marwick LLP, 99 High Street, Boston, MA 02110, USA.

Today, biometric systems are being widely developed and deployed to provide greater security to users and there is an increased awareness of the value of biometric systems. Biometric systems are being developed and deployed, users are gaining experience and confidence in biometric systems and are beginning to reap the benefits of this technology. Users and developers of this technology have also recognized the need for a biometric standard and work on a defining standard is currently underway. The standard establishes an appropriate biometric model and the associated security requirements that will allow different biometric solutions to co-exist in the marketplace. The standard views biometric systems within a global user community and it assures that the security of any one biometric system will be unaffected by the security of any other biometric system. This paper argues that integrity of authentication data is the primary security requirement and that confidentiality is secondary, even though the majority of authentication schemes today encrypt PINs and passwords.

Background

When Alice logs onto a system (host computer or workstation), how does the system know it is Alice and not, say, Eve, who is trying to impersonate Alice? Basically, there are three ways in which she can be authenticated to the system:

1. On the basis of something Alice *knows*, e.g. password or Personal Identification Number (PIN), called a *knowledge factor*.
2. On the basis of something Alice *has*, e.g., a magnetic strip card or a secret key stored on a smart card, called a *possession factor*.
3. On the basis of something Alice *is*, such as a measurable biological or behavioural characteristic, that reliably distinguishes one person from another and that can be used to verify or recognize the claimed identity of the person, called a *biometric factor*.

Further discussion can be found in the ANSI standard X9.49 [1, §6. *Entity Authentication*].

Biometrics are fast emerging as a reliable automated method of establishing the identity of a living person, such as an ATM customer or computer user. Examples of biometrics include finger, voice, iris, face and hand. The single data representation of a biometric characteristic or measurement, captured or scanned by a biometric device is called a *biometric sample*. The information extracted from one or more biometric samples is used to create a *biometric template*. An individual is authenticated when the *biometric sample* is found equivalent, or 'matches' with the *biometric template*. Both the *biometric sample* and the *biometric template* are called *biometric data*, or *biometric information*. An automated system capable of collecting, distributing, storing and processing biometric data and returning a decision (match or non-match), is called a *biometric system*. A biometric system is comprised of the biometric data necessary to perform user verification or user identification and the software and physical hardware required to collect, distribute, store and process the biometric data.

Computerized biometric devices have been available since the early 1970s, although biometric technology did not emerge as a practical means of identifying computer users until recently. The factors responsible for this change are:

- Today, biometric technology is more accurate.
- Biometric devices are more reliable and durable.
- Biometric systems are more affordable.

Overview of Biometric Technology

Biometric identification exploits the universally recognized fact that certain physiological or behavioral characteristics reliably distinguish one person from another. Biometrics includes both the automatic collection and the comparison of these characteristics. The digital representations of these characteristics are stored in an electronic medium and later used to confirm the identity of an individual. A typical authentication process utilizing biometric technology consists of the following basic steps:

1. Capture the biometric data.
2. Evaluate the quality of the captured biometric data and recapture if necessary.
3. Process the captured biometric data to create a biometric sample.
4. Match the biometric sample with a previously enrolled template, or templates, to determine if a match exists. This matching can be done as verification or identification.

Verification is a process in which a biometric sample is compared with a particular, previously generated biometric template, stored in a database or on an ID card, in order to verify the correctness of the user's 'claimed identity'. Verification involves a 'one-to-one' comparison. The biometric template is retrieved from the database using the user's claimed identity, e.g. user ID, user name, etc., or is assumed based on the user's possession of the ID card containing the biometric

template. If the biometric sample matches the previously generated biometric template, the claim of identity is confirmed or verified.

Identification is a process in which a biometric sample is compared with all of the biometric templates, or a subset based on search algorithms, in the database in order to find a matching template and thus identify the person who provided the biometric sample. Identification involves a 'one-to-many' comparison. Unlike verification, the user does not provide a 'claimed identity', but instead is identified strictly on the basis of the biometric sample matching one of the biometric templates in the database. The technique can be used for recognition or to confirm that the person being identified is not known under a different name.

Enrolment is the process of entering a new biometric template and identifier into the database. It is usually entered along with other information about the individual, which links them to an organization, an account, or a set of privileges. Enrolment can incorporate identification to make sure that the individual is not already in the database, perhaps under another name. If no match is found, the biometric template, the identifier and its associated information can be added to the database.

Biometric techniques are subject to statistical error. The probability that a biometric system will incorrectly identify an individual or will fail to reject an imposter is historically deemed 'false acceptance'. The probability that a biometric system will fail to identify a person enrolling in the system, or verify the legitimate claimed identity of someone who has already enrolled is historically deemed 'false rejection'. False acceptance occurs when a person's biometric is scanned and accepted by the system, when in fact it should not have been accepted. False acceptance is also called 'False Match' (FM), i.e. failure to reject an imposter and false rejection is also called 'False Non Match' (FNM), i.e. failure to accept a bona fide individual (see *Figure 1*).

All biometric technologies inherently suffer from some level of False Match or False Non Match. The

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

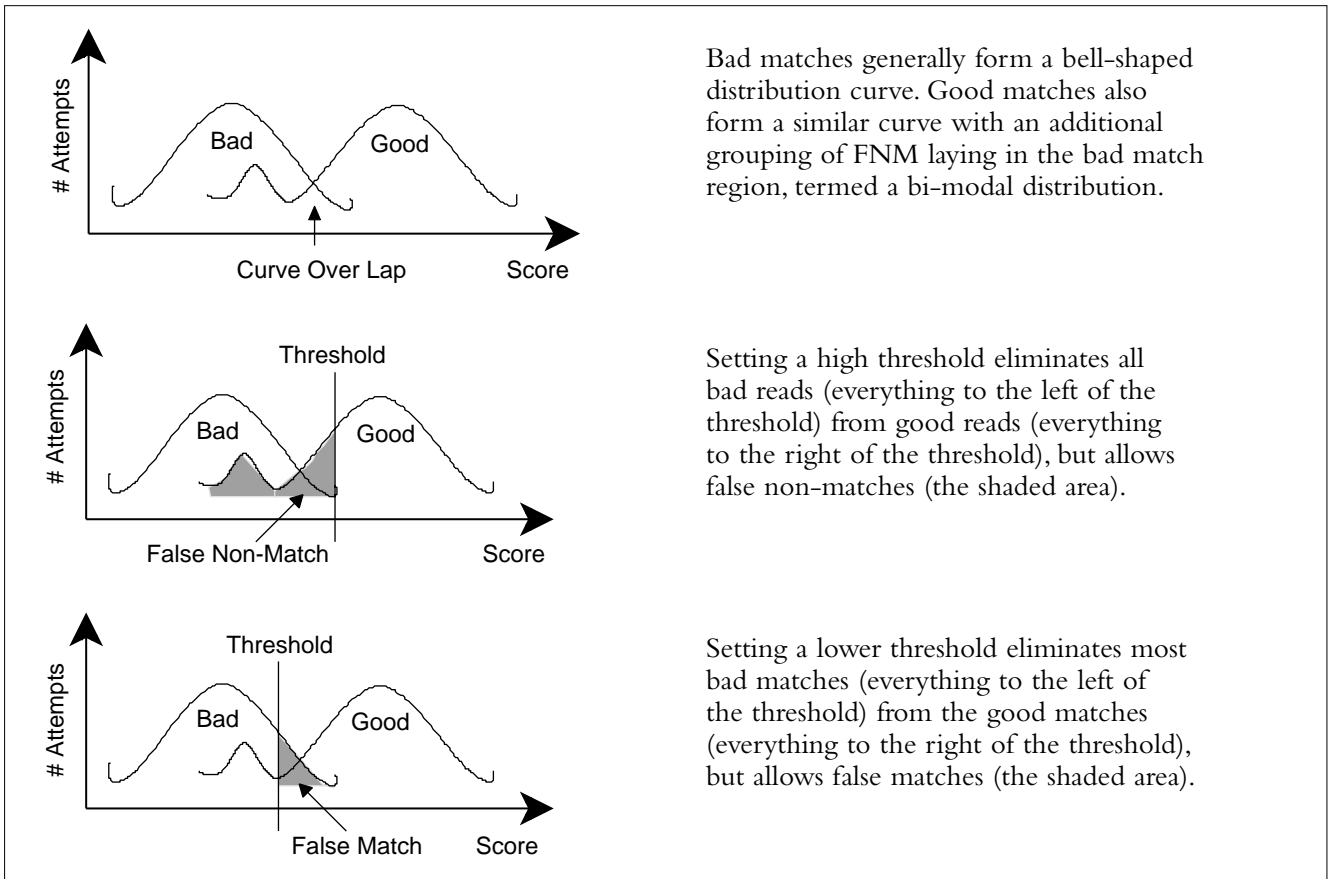


Figure 1: Distribution Curves.

relationship between False Match and False Non Match values for any particular biometric is an inverse one. Thresholds of acceptance for any particular biometric data are set according to the needs of the organization. For example, a high security facility will usually minimize the False Match rate at the expense of increasing False Rejection rate, whereas a customer service facility will usually minimize False Non Match rate at the risk of increasing the False Non Match rate.

The Need for a Biometric Standard

Business practice has changed with the introduction of computer-based technologies. The substitution of

electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate alteration, substitution or destruction of data. This risk is compounded by interconnected networks and the increased number and sophistication of malicious adversaries.

Some of the conventional 'due care' controls used with paper-based transactions are unavailable in electronic transactions. Examples of such controls are safety paper which protects integrity and handwritten

signatures or embossed seals which indicate the intent of the originator to be legally bound. In an electronic-based environment, controls must be in place to provide the same degree of assurance and certainty as in a paper environment. Secure digital verification schemes are increasingly important. Security applications will soon require verification based on biometrics, rather than solely on PINs or secret keys. The need for a biometrics' standard to guide the financial services industry in the management and security of biometric systems is of paramount importance.

ANSI Standard X9.84, *Biometrics Management and Security* [2] — under development in one of the ANSI standards groups — is intended to fill this present need. The Standard describes adequate controls and proper procedures for using biometrics as an identification and/or authentication mechanism for secure remote electronic access or local physical access controls for the financial services industry. But, the standard will have broader applicability to general commercial (non-financial) applications, as well.

The Standard addresses the following issues:

1. Security for the collection, distribution and processing, of biometrics data, encompassing data integrity, authenticity and non-repudiation.
2. Management of biometrics data across its life cycle, comprised of the enrolment, transmission and storage, verification, identification, and termination processes.
3. Usage of biometrics technology, including one-to-one and one-to-many matching, for the identification and authentication of banking customers and employees.
4. Application of biometrics technology for internal and external, as well as logical and physical access control.
5. Encapsulation of biometrics data.
6. Techniques for the secure transmission and storage of biometrics data.

7. Security of the physical hardware used throughout the biometrics data life cycle.
8. Techniques for integrity and privacy protection of biometrics data.

The standard presents a technology framework in which the previous topics are addressed. There are several issues that the Standard does not address. The Standard does not address the individual's privacy and ownership of biometric data. Nor does it address application specific requirements and limitations for employing biometric technology. The Standard does not recommend biometric technology. These are considered outside the scope of the Standard. However, the developers of the Standard are tracking the potential impact of the European Union Privacy Directive (effective October 1998), and US legislation, such as the Healthcare Insurance Portability and Accountability Act (HIPAA 1996), in case they have technical ramifications that might influence the development of a biometric standard.

Biometric Technology Framework

All biometric systems are composed of the following subsystems:

- data collection
- transmission

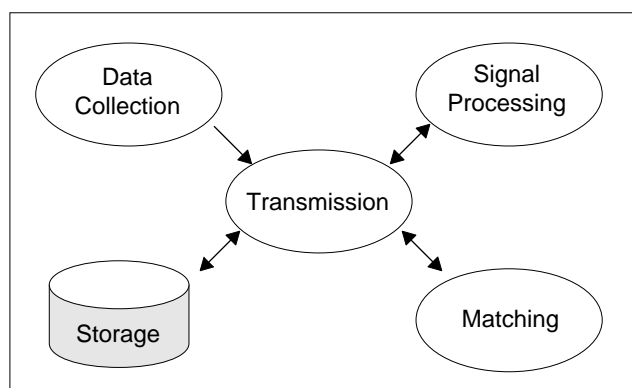


Figure 2: Major Subsystems of a Generalized Biometric Architecture.

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

- signal processing/feature extraction
- matching
- storage

Figure 2 shows the general biometric system model. In some biometric systems the feature extraction is simply a passthrough of the data obtained in the data collection subsystem, however, all other components are necessary. Each subsystem is described in detail in the sections that follow.

The Data Collection Subsystem

The data collection subsystem contains the input device or sensor that reads the biometric information from the user and converts it to a form suitable for processing by the remainder of the biometric system. It is the link from the physical domain to the logical domain. Examples include a variety of transducers such as a video camera, a fingerprint scanner, a special signature pen or tablet, a microphone and other input devices specific to the chosen biometric characteristic to be measured. The output of this subsystem is raw biometric data, which may be processed locally, or may be transmitted to another location.

The sampled biometric characteristic must always be similar to the user's enrolled template to which it is compared. This imposes requirements on the design of the data collection sensor and may impose training requirements for the users. Some characteristics change slowly over time and biometric systems may employ *adaptation* in order to keep the stored reference template in step with those changes. The selected biometric characteristic must be one that is not expected to change often or to a large degree as compared to the interval of renewal or adaptation of the template. Renewal is the re-enrolment of a user by provision of a new enrolment template for that individual. This may occur on a time interval basis, or is event driven, such as in the case of biometric systems that carry out an adaptation process.

In use, the biometric feature is presented to a sensor, which converts the feature into an electronic signal

suitable for further processing. All sensors in a given system must be similar enough that a feature measured by one sensor will closely match the same feature measured at other sensors, so that the user can be recognized equally well at any location. This includes the requirement that the sensors must be consistent over time, either by virtue of inherent stability, or through use of automatic calibration. Some systems include automatic quality control features in the sensors or signal processing paths, and these systems can detect poor quality signals that might otherwise increase the false reject rate.

The performance and output of the data collection subsystem is impacted by changes in any of the following.

- The underlying biometric pattern.
- The presentation of the pattern to the sensor.
- The performance of the sensor itself.

Changes in any of these will result in increased recognition errors.

The Transmission Subsystem

The transmission subsystem provides the ability to send information between the Data Collection, Signal Processing, Decision, Storage and matching components. The connectivity provided may be point-to-point or networked, allowing one system to connect to multiple subsystems. The system components that are communicating may be local or remote to each other, within the same secure envelope (e.g. tamper-resistant secure module¹) or in separate secure envelopes. The transmission subsystem may not necessarily be monolithic, but may actually be composed of a number of different transmission mediums such as Ethernet, leased line, wireless, etc. These media may or may not provide security services such as confidentiality integrity and authentication between the connected subsystems.

¹ See X9F6 draft standard x9.68-20xx and FIPS 140-2 for a definition of the requirements for tamper-resistant security modules.

The Signal Processing Subsystem

The signal processing subsystem receives the raw biometric data from the sensor, and transforms that data into the form required by the pattern matching stage. The exact processing that takes place varies for different biometric characteristics that are measured and for different vendors' biometric systems. Some representative processing steps are described below.

- The system may perform a quality analysis on the input signal to determine if it is satisfactory for use. If the signal fails the quality tests, it is rejected and the user must supply another sample.
- Filtering may be applied to the signal in order to remove noise or other information that is extraneous to the matching process. This may include, for example, removing high or low frequency data from the signal.
- The signal may be normalized in some way. For example, the voltage level of an analogue signal may be adjusted to be within accepted limits and a video image may be adjusted to standard levels of brightness or contrast.

Once the input signal has been adjusted so it is satisfactory, it may be analyzed to extract features that are used by the matching subsystem. Some biometric systems compare raw data and this step is not required. For most systems, however, feature *extraction* is performed to transform the raw data into a set of characteristics that will represent it to the matching process. The types of features vary with different biometric techniques. A fingerprint system typically looks for physical characteristics such as branch and end points of the ridges; the system would extract a set of values, where each one contained an indication of the type of feature found and the coordinates where it was found on the finger. A voice recognition system, on the other hand, might record such things as the magnitude of signal found in different frequency ranges. The result of feature extraction is usually data that is much smaller and simpler to use than the original raw data signal.

Matching Subsystem

The matching subsystem has a key role in the biometric architecture. The matcher is composed of the following sub-components:

- a sequencer
- a match scoring module
- an adaptation module (optional)
- a decision module

The sequencer handles the sequencing of the activation of the match, adaptation and decision modules to perform different functions.

The match-scoring module measures the similarity of a test sample with a template. Each comparison of a sample with a particular template yields a *score*, which is a numeric value indicating how closely the sample and template match. The method of computing the score differs among biometric technologies, but typical methods include distance metrics², probabilistic measures, and normalized correlation. Ultimately, the score should correspond to a given confidence of positive identification for the biometric subject which can be factored into the overall business rules and risk policy for the financial institution authorization policy. Ultimately this confidence value will be considered in the authorization policy for the transaction employing the biometric as an identification factor.

In the simplest form of verification, the sequencer provides the claimant and enrolment templates to the matcher and passes this result to a decision module, which returns a binary decision regarding whether the claimant is who they claim to be.

However, the interplay between the match scoring module and the sequencer may be quite involved in systems that carry out identification. For example, in an identification mode, the sequencer may take into

² See Jain, Pankanti et al., *Personal Electronic Identification in a Networked Society*, Kluwer, 1999.

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

account additional indexing information about the claimant template in order to focus the computations of the matcher onto templates that are most likely to match the claimant template. The decision module might also be invoked during the identification process to guide the search towards the likeliest match enrolment templates.

Some systems use the sequencer, matcher and decision module to perform adaptation to keep the enrolment templates up-to-date with gradually changing biometric characteristics for the user.

The decision subsystem returns a binary yes or no regarding the positive identification of the claimant on the basis of the score computed by the pattern matching subsystem. In the most common case, the decision is based on a single threshold. If the score is above the threshold, the system concludes that the user is indeed the individual owning the template. If not, the system indicates that the user is not that individual.

An application program, for example, a transaction authorization system, uses the decision process result. It may be used in various ways, depending on the purpose of that application program. The actions at this level are not a part of the decision subsystem itself, but are a part of that application program. Most often, the application program will grant the user some level of privilege if the decision indicates a match with the template belonging to the claimed identity. In other systems, however, the goal is to verify that the user is not in the template database — for example, when an individual attempts to enroll in a benefits program. In this case, the application program will ‘accept’ the user only if the decision subsystem indicates that there are no matches between the user’s sample and any template in the current database.

The Storage Subsystem

The storage subsystem maintains the templates for the enrolled users. It provides for the addition, deletion and retrieval of an enrolled template (or templates) as needed by the matching subsystem. The storage subsystem may contain a single template for a single user or thousands of templates depending on the system

architecture and intended function. For example, templates may be stored:

- In physically protected storage within the biometric device.
- In a conventional database on a computer system.
- In portable tokens, such as smart cards.

The data stored for each user always includes that user’s template, but it may also include other information. It may also be data that is completely unrelated to the biometric system, if the same database is used for purposes other than user authentication.

Security Issues

The most controversial aspect of the new biometric Standard is the security requirements adopted by its developers. A central issue facing the Standard’s developers was whether biometric data should be treated as secret data, like a PIN or a private key, or whether it should be treated as public data, like an identifier or a public key. The Standard’s developers were likewise cognizant that even experts in the field of biometric research and development had not yet reached a consensus on this issue.

A paper by Davida et al. [3] discusses offline identification protocols in two environments: (1) identification using public biometrics, with no requirement to hide one’s biometric, and (2) identification using private biometrics. The authors take no position as to which environment is preferred, but they do raise arguments that question the acceptability of a solution based on private biometrics. For example, one may argue that the assumption of privacy is not acceptable, especially against a strong adversary with sufficient motivation and resources. They point out that a key derived from a private biometric is a lifetime key that cannot be revoked easily. And they point out that, under certain conditions, scalability in a system using private biometrics can be a problem.

A paper by Kim [4] discusses the drawback of using private biometrics, but stops short of recommending

the use of public biometrics. The following is a direct quote:

“The fact that most physiological characteristics are almost impossible to alter, introduces another drawback to the use of biometric systems. For example, assume that a biometric system is being used for controlling access to a remote computer and that the user templates are stored on that computer. When a user who wishes to log on, enters his/her user identity at the terminal, the biometric measurements are transmitted to the host for comparison. This procedure would introduce at least two important potential weaknesses in the system: one relates to the database with the templates and the other to the transmission of the biometric reading. If an impostor were able to obtain either of these items of information, he/she could then impersonate that user. If this was to happen then it would be difficult to invalidate fraudulent claims and to protect the genuine user, as the user cannot easily change a ‘biometric password.’ This is a definite disadvantage compared with a conventional password based system where the user can easily change the password if it is felt to have been compromised. In fact, this can go further. For example, if the fingerprinting method is used and a user wants to access several computer systems, the danger of fraudulent access can be accelerated if any one of those systems is careless regarding either the transmitting or the storing of the templates. An impostor might get hold of information from one weak system that he/she can use to falsify the identity on all the other systems. Again since there is no (easy) way to change a user’s fingerprint, it is a far more serious problem than the simple disclosure of a user’s password or the misplacement of an ID card.”

A paper by Schneier [5] discusses the strengths and weaknesses of biometrics and suggests that a trusted path is necessary. The following are excerpts from the paper:

“Biometrics are great because they are really hard to forge: it’s hard to put a false fingerprint

on your finger, or make your retina look like someone else’s.”

“Biometrics are lousy because they are so easy to forge: it’s easy to steal a biometric after the measurement is taken.”

“They [biometrics] are useful in situations where there is a trusted path from the [biometric] reader to the verifier.”

However, experts in the field of biometrics generally agree on the following points:

- A. Biometric data can be captured anywhere. Fingerprints can be lifted, faces and eyes can be photographed, voices can be recorded, DNA can be covertly obtained, etc. One cannot stop an adversary from collecting biometric data outside the system.
- B. In a system based on private biometrics, it is possible, over time, for a user’s biometrics to be compromised (no fault on the user’s part) and for the user to be permanently barred from access to the system based on his biometric data. Is this what we call ‘stealing someone’s identity’?
- C. It is reasonable to assume that there is a non-negligible probability that given sufficient money and expertise, Hollywood-type special effects could be used to create a synthetic biometric that could subvert a biometric device.

For these reasons, the Standard’s committee adopted the following basic security axiom: “The security of a biometric system cannot rely on keeping biometric data secret (e.g. through encryption).” This has two important consequences:

1. Because the biometric data is treated as public data, the security requirements are adjusted to ‘take up the slack’, so-to-speak, so that a biometric system will provide the highest possible protection. Thus, the integrity of biometric data is (or becomes) the strongest requirement.

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

2. Since maintaining the secrecy of biometric data is not achievable, it establishes practical limits on the degree of protection that one can reasonably expect to achieve using biometrics.

Of course, there are other valid reasons to protect the secrecy of biometric data (e.g. via encryption). These include privacy, liability issues and intellectual property issues. For example, a vendor may have a unique algorithm for generating biometric templates that it wishes to keep proprietary.

The Standard discusses two distinct types of authentication systems employing biometric technology, open systems and closed systems. *Table 1* compares software, hardware, and data characteristics between the two systems.

A closed system is one in which information is kept proprietary and not shared outside the system. In fact, the security afforded by a closed system, in general, depends on maintaining the secrecy of (1) details of the biometric system, (2) identities of users, (3) biometric data, or (4) some combination thereof. In general, a closed system is one under the control of a single enterprise, with a limited, well-defined set of users.

An open system is one in which information can be shared with other systems. An open system is one in which there is no loss in security if (1) the same biometric technique is implemented in many different systems and vendor products and (2) users are authenticated by many different systems using the same biometric technique. An open system is one in which the

Characteristic	Closed (proprietary) System	Open System
Software	<p>Knowledge of what biometrics are used (e.g., fingerprint, voice, iris) is kept proprietary or secret.</p> <p>Users are prohibited from using the same biometric technique and biometric data, in different systems.</p>	<p>Knowledge of what biometrics are used is treated as non-sensitive or public information.</p> <p>Users are allowed to make use of the same biometric technique and data across many different systems.</p>
Hardware	<p>Biometric readers are located in private and controlled spaces.</p>	<p>Biometric readers are located in public places.</p>
Data	<p>Biometric information is not shared outside the system, because doing so could diminish or potentially compromise the system</p> <p>Biometric information is kept confidential and thus must be encrypted when transmitted over communication lines and/or in storage.</p> <p>Biometric information becomes invalid when a user's biometric data has been disclosed in an unauthorized manner.</p>	<p>Biometric information is shared among many biometric systems under the control of different organizations and across different jurisdictions.</p> <p>Biometric information is treated as non-secret data and hence encryption is unnecessary when transmitted or stored for reasons of confidentiality.</p> <p>Unauthorized disclosure of a user's biometric data does not invalidate the biometric information.</p>

Table 1: Closed versus Open Systems.

quality of protection afforded by one system is independent of the quality of protection afforded by any other system. Hence, the security in a well-designed system will be unaffected by the lack of security in a poorly designed system implementing the same biometric technique. In general, an open system is capable of providing protection even when implemented across many enterprises and within many different products, possibly using the same biometric technique, and one capable of supporting a heterogeneous community of users with no direct relationship to the enterprises that own or manage the system.

Security Requirements

In this section, we list the security requirements for a biometric system and provide the rationale for each security requirement.

Injection of False or Replayed Biometric Data

An attacker might attempt to subvert security by capturing biometric data that is later injected into the system, thereby allowing the attacker to masquerade as the individual whose data was captured. The attack could be perpetrated in several different ways.

Eve might attempt to subvert security by attaching a fake biometric capture device to the system. Unlike a genuine device, which performs actual biometric measurements, the fake device would merely provide a portal for inputting captured biometric data; it wouldn't actually perform biometric measurements. Potentially, a fake device would allow Eve to input Alice's captured biometric data, as if it were her own and hence masquerade as Alice.

Requirement 1: *The biometric system must prevent captured biometric data from being introduced into the system through fake, system-attached, biometric capture devices.*

The origin of sample data at the point of capture must be authenticated. This is akin to a POS terminal where a unique secret value is necessary to authenticate the device. This is typically a symmetric key used

for either encryption and/or MACing, or an asymmetric private for a digital signature.

The requirement can be met if each device contains a (device or system) secret value that can be used to authenticate the source of sampled biometric data, when the data is transmitted from one device to another within the system. For example, the secret value could be a private signature key used to sign the sampled biometric data or it could be a symmetric key used to generate message authentication codes (MACs) on the sampled biometric data.

In alternative form of the attack, where sampled biometric data is transmitted from one device to another over an exposed communication link, Eve can masquerade as Alice by using a valid biometric capture device in combination with an active 'line tap'. In this case, the biometric capture device reads Eve's biometric sample, but Eve enters Alice's user identifier (userID) instead of her own userID. Then, Eve performs an active 'line tap' causing her sampled biometric data to be replaced by Alice's captured biometric data. Although this is a more 'high-tech' attack, it is clearly 'do-able' using existing technology.

A similar attack could be launched if Eve were able to intelligently modify the templates controlled by the system. Eve could masquerade as Alice by merely replacing Alice's template with her own (Eve's) template. Likewise, if templates are transmitted from a central location to another device where verification is performed, then Eve could masquerade as Alice by performing an active 'line tap' and replacing Alice's template with her own (Eve's) template.

Requirement 2: *The biometric system must ensure that biometric data can be introduced into the system only through authorized interfaces using prescribed procedures. In effect, this means that the system must protect the integrity of its biometric data, including biometric samples and biometric templates. It must not be possible for an attacker to replay intercepted biometric data, or inject biometric data into the system (e.g. via an active line tap), or replace stored or transmitted biometric data, including biometric samples and biometric templates, with biometric data specified by the attacker.*

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

The requirement could be met, if the entire system is contained within a single tamper-resistant module. In that case, one could argue that physical security alone will suffice to ensure data integrity. However, if any two system components have a transmission between them (unless one can offer a completely shielded cable under constant physical inspection), then some form of cryptographic protection is required, namely a MAC or digital signature.

Synthetic Biometric Feature Attack

An attacker fabricates an analogue of the real user's biometric characteristic, using captured information. The fabrication is subsequently used to impersonate the user to the biometric system. It is impractical to prevent collection of biometric information from an individual and so the preventive measures apply to the possible use of the fabricated analogue of the user's biometric characteristic. For example, facial features could be captured from a photograph, a fingerprint could be obtained from a water glass. Biometric samples and biometric templates transmitted within the system could be intercepted by an adversary. An adversary might be able to access and read the templates stored within a template database. An attacker might install fake biometric readers that unsuspecting users believe are part of a real system. The fake readers would collect all the biometric samples entered through these readers.

Obviously, encryption is not the 'answer' to the synthetic biometric feature attack. At most, encryption can protect biometric information stored or transmitted within the system. It cannot stop an attacker from obtaining biometric information outside the biometric system, e.g. from photographs, or lifted fingerprints, or using fake biometric readers. Because it is impractical to prevent collection of biometric information from an individual, we argue, therefore, that preventative measures (defending against the synthetic biometric feature attack) apply to the possible use of the fabricated analogue of the user's biometric characteristic.

Requirement 3: *The biometric system must implement protection mechanisms (controls and procedures) to detect or deter the synthetic biometric feature attack.*

The requirement can be met by fabricating biometric capture devices that detect synthetic biometric features, e.g. fingerprint readers that detect warmth and pulse. Electronic monitoring by means of a video camera would act as a deterrent and assist law enforcement officials in identifying perpetrators.

Exposure or Loss of Biometric Data

A biometric system may be required to protect the confidentiality of biometric data in order to comply with existing privacy laws, or to achieve liability protection, or to protect a vendor's intellectual property. NOTE: The system does not need to protect the confidentiality of biometric data in order to ensure the integrity and accuracy of the biometric recognition system itself.

Requirement 4: *Where necessary, the biometric system must implement protection mechanisms (controls and procedures) to prevent the exposure or loss of biometric data.*

The requirement can be met by encrypting biometric information to prevent its unauthorized disclosure, or by maintaining biometric information within a physically secure environment (e.g. a secure module), or a combination of both.

Registration of Individuals Using False Identities

Each user must prove his or her identity to the biometric system owner before being allowed to enroll. This provides assurance that the biometric reference template is actually bound to the identity of the individual who enrolled and not to a different person, who the enrollee might claim to be. Security is compromised if any individual can enroll using a false identity.

Requirement 5: *The biometric system must implement protection mechanisms (controls and procedures) to ensure that the enrollment process is a well-defined and controlled process and one that will prevent registration of individuals using false identities.*

Finding Collisions

A biometric collision occurs when the template value for one user, say i , is ‘close enough’ to the template value for another user, say j , such that biometric samples for user i are authenticated with the template for user j with some reasonable probability.

In one form of the attack, the attacker attempts to verify his biometric characteristic against any one of a large number of templates in the system database. In this case, the attacker is attempting to find one or more other individuals whose biometric data is similar enough that he can successfully verify himself as any of those other people. This is a possibility with many biometric technologies: any non-zero false accept rate indicates that there will be individuals who can verify against each other’s templates. The attack could be perpetrated either by first obtaining a copy of the template database and then performing the attack on a machine under the control of the attacker, or it could be perpetrated via a trial-and-error attack using system-designed interfaces. In the latter case, the attacker would repeatedly attempt to be authenticated with his biometric sample, but using the IDs of different users.

In a related attack, the attacker tries to find a template that matches a selected person’s biometric data. The attacker might choose a person with a high level of authority or other characteristic that makes them an attractive target. The attacker tries to find a template that matches the target person. If one is found, he attempts to collude with the owner of the matching template in order to defraud the target person. In yet another related attack, the attacker looks for matches between any two templates in the database. If two sufficiently similar templates are found, the attacker attempts to convince one of the two people to collude in defrauding the other person in the matching pair. Both of these related attacks require that the attacker have access to the template database or to have the means to reconstruct a significant portion of the database. It might be possible to reconstruct a portion of the database by intercepting templates transmitted within the system, or by intercepting biometric samples and computing the templates from the samples.

Requirement 6: *The biometric system must restrict access to the template data; it must restrict the ability of an attacker to reconstruct the template database from intercepted biometric data (samples or templates); it must restrict the ability of an attacker to issue verification requests against data in the template database.*

A number of countermeasures can be used to meet this requirement. The storage system can restrict access of biometric templates to authorized personnel and appropriate applications. The storage system can record in an event journal all authorized and unauthorized attempts to add new templates, modify existing templates, or delete templates. The storage system can track the number of accesses to each template and can trigger an alarm whenever a tolerance threshold is exceeded. The storage system can record the following information in an event journal: (1) threshold tolerance alarm (2) access summary information on a periodic basis (3) addition, modification and deletion summary information on a periodic basis. The system might also save the biometric samples associated with failed authentication attempts. Periodically, the system could look for biometric samples that match and if too many of the biometric samples are found to match each other, the system might conclude that it is being attacked by a single attacker who is trying to verify his biometric characteristic against any one of a large number of templates in the system database.

Ongoing Biometrics Standardization and Related Activities

ANSI X9F4 *Cryptographic Applications* — the working group developing ANSI Standard X9.84 *Biometric Information Management and Security* [2] — is one of several working groups operating under the X9F *Data and Information Security* subcommittee. X9F is one of several subcommittees within the Accredited Standards Committee (ASC) X9 [6], and is accredited by the American National Standards Institute (ANSI). X9 develops and publishes voluntary, consensus technical standards for the financial services industry. X9’s inter-industry voting membership includes over 300 organizations representing investment managers,

A Biometric Standard for Information Management and Security

/S. M. Matyas Jr & J. Stapleton

banks, software and equipment manufacturers, printers, credit unions, depositories, government regulators, associations, consultants and others.

The X9F4 working group has nearly three dozen active members, comprised of six large financial institutions and associations, almost a dozen vendors offering security-related products and services, half a dozen biometric vendors and consultants and others. The working group has existed for over five years and its prior work includes the ANSI standard X9.49 *Secure Remote Access to Financial Services* [1].

The X9F4 working group has also established liaisons with other biometric-related industry groups and other standards organizations, including:

- The BioAPI Consortium [7]. The BioAPI Consortium is a group of over 35 organizations that have a common interest in promoting the growth of the biometrics market. BioAPI is dedicated to developing a specification for a standardized Application Programming Interface (API) that will be compatible with a wide range of biometric applications programs and a broad spectrum of biometrics technologies. The API description defines how application programmers and biometric solution vendors write to the common BioAPI interface. The BioAPI runtime framework will allow applications to interoperate with various biometric solutions. The Consortium was formed to develop a widely available and widely accepted API that will serve for various biometric technologies.
- The International Biometric Industry Association (IBIA) [8]. The International Biometric Industry Association (IBIA) is a trade association founded in September 1998 in Washington, DC, to advance, advocate, defend and support the collective international interests of the biometric industry. IBIA is governed by and for biometric developers, manufacturers and integrators, and is impartially dedicated to serve all biometric technologies in all applications. The IBIA is the official registrar for X9.84 object identifiers and the BioAPI identifiers, which can be found at www.ibia.org/formats.htm.
- The ANSI B10 committee for Drivers Licenses/ Identification [9]. ANSI B10.8 Driver's License/ Identification Card Standard, through ANSI's Accredited Standards Committee, National Committee for Information Technology Standards (NCITS), is a committee dedicated to identification cards and related devices known as B10. A Working-Group was formed in B10 for driver's license/identification cards (DL/ID) and designated B10.8. The Working-Group is comprised of industry (vendors) and jurisdictional representation (AAMVA's members). The development involves broad-based project teams including state driver license agencies, government, equipment and software suppliers, card vendors and consultants.
- The Joint Technology Committee (JCT1) Subcommittee 17 (SC17) Identification Cards And Related Devices [10]. JCT1 / SC 17 is a joint subcommittee of the ISO and IEC organizations, whose scope includes integrated circuit card with contacts, financial transaction cards, optical memory cards and devices and motor vehicle driver's license and related documents. SC17 has initiated a new work item to establish the data and file structures for storing biometric templates in smart cards.
- The NIST/ITL Common Biometric Exchange File Format (CBEFF) working group. The National Institute for Standards and Technology (NIST) Information Technology Laboratory (ITL) has sponsored several workshops to establish an industry specification that defines a common biometric exchange format (CBEFF) and associated metadata that will enable interoperability of biometric-based application programs and systems from different vendors.
- The Biometric Consortium [11]. The Biometric Consortium serves as the US Government's focal point for research, development, test, evaluation and applications of biometric-based personal identification/verification technology. It is currently co-managed by two US Government agencies: the National Institute for Standards and Technology (NIST) and the National Security Agency (NSA).

- The ISO Technical Committee 68, Subcommittee 2 (SC2) Security Management and General Banking Operations [12]. The Subcommittee's scope is to facilitate banking and related financial operations including codes, banking procedures and related security standards.

The purpose of these liaisons is to share information across multiple disciplines and to foster understanding between disparate organizations that are all working toward furthering biometric technology. The X9F4 working group plans to conduct a pre-ballot review of the standard with all of the liaison groups.

Outlook for the New Standard

ANSI draft standard X9.84 — developed by the X9F4 working group — will be ready for balloting in X9 in mid-2000, with a customary 60-day comment period to follow shortly thereafter. The X9F4 working group expects to coordinate the ballot process with its liaison groups to ensure acceptance of the best possible standard. Afterwards, the Standard may be submitted to ISO for consideration as a new international standard.

Acknowledgements

Portions of this paper are based on text from working drafts of the X9.84 standard. The authors wish to express their appreciation to the X9 Accredited Standards Committee, the X9F Data and Information Security subcommittee, and in particular its previous chair, Glenda Barnes, for their support. The authors also wish to recognize the X9F4 working group and particularly the editors and writers of X9.84, for their contributions: Todd Arnold, Phil Griffin, Mort

Hoffman, Sandra Lambert, Judith Markowitz, Ron O'Connor, Pud Reaver, Marcos Salganicoff, Ed Scheidt, Rena Smith, and Richard Yen. Finally, the authors wish to especially recognize Dr John Colombi, Captain USAF, for his contributions.

References

- [1] ANSI X9.49-1998 *Secure Remote Access to Financial Services*, American Bankers Association, secretariat.
- [2] Draft X9.84-199x *Biometric Information Management and Security*, Accredited Standards Committee X9F4 Working Group.
- [3] George I. Davida, Yair Frankel, and Brian J. Matt, "On enabling Secure Applications Through Off-line Biometric identification," *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 1998, pp. 148-157.
- [4] Hyun-Jung Kim, "Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control?", *Computers & Security*, Vol. 14, No. 3, 1995, pp. 205-214.
- [5] Bruce Schneier, 1998. "Biometrics: Truths and Fictions," *Crypto-Gram*, 15 August 1998: www.counterpane.com/crypto-gram-9808.html - biometrics.
- [6] ASC X9 Committee: www.x9.org.
- [7] BioAPI: www.bioAPI.org and/or www.bioapi.com.
- [8] International Biometric Industry Association (IBIA): www.ibia.org.
- [9] ANSI B10.8 working group for Drivers License / Identification: www.aamva.org.
- [10] ISO Joint Technical Committee 1 (JCT1) Subcommittee 17: www.iso.ch.
- [11] Biometric Consortium: www.biometrics.org.
- [12] ISO Technical Committee 68 (TC68) Subcommittee 2: www.tc68.org.