National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Biometrics Frequently Asked Questions

Introduction

This set of Frequently Asked Questions (FAQs) was developed by the National Science & Technology Council's (NSTC) Subcommittee on Biometrics with the full understanding that national (INCITS/M1) and international (ISO/IEC JTC1 SC37) standards bodies are working to develop standard references. The subcommittee will review this set of FAQs for consistency as standards are passed. The subcommittee recognizes the impact of ongoing challenge problems, technical evaluations, and technology advancements. The FAQs will be updated accordingly to reflect these changes. The statements herein are intended to further the understanding of a general audience and are not intended to replace or compete with sources that may be more technically descriptive/prescriptive.

Top 10 Biometric FAQs

Q1: What is "biometrics"?

Biometrics is a general term used alternatively to describe a characteristic or a process.

- As a characteristic: a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- As a process: a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Q2: What are the common biometrics?

Biometrics commonly implemented or studied include fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment.

Q3: Which biometric technology is the best?

There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity. For example, fingerprint recognition has been used for over a century while iris recognition is a little more than a decade old. It should be noted that maturity is not related to which technology is the best, but can be an indicator of which technologies have more implementation experience.

Q4: How are biometrics collected?

Biometrics are typically collected using a device called a sensor. These sensors are used to acquire the data needed for recognition and to convert the data to a digital form. The quality of the sensor used has a significant impact on the recognition results. Example "sensors" could be digital cameras (for face recognition) or a telephone (for voice recognition).

Q5: What are biometric templates?

A biometric template is a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors. Not all biometric devices are template based. For example, voice recognition is based on "models." The difference between templates and models is beyond the scope of this paper.

Q6: What is the difference between recognition, verification and identification?

- *Recognition* is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled.

- *Verification* is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

- *Identification* is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

"watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database.

Q7: Where are biometric technologies currently being deployed?

Biometrics are being used in many locations to enhance the security and convenience of the society. Example deployments within the United States Government include the FBI's IAFIS, the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. These deployments are intended to strengthen the security and convenience in their respective environments. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks.

Q8: Can I interact with a biometric device without touching something?

This depends on the specific modality being used. For example, with today's current technology, an individual would be required to touch a fingerprint sensor for the system to obtain the biometric sample, whereas face imaging for face recognition and iris imaging for iris recognition are contactless and would not require the user to touch the system.

Q9: Can I interact with a biometric device without touching something?

Biometrics is a security tool available for use. An environment or circumstance may or may not need a biometric system, depending on the application. To determine if a biometric is needed, one must understand the operational requirements of the situation. Biometrics should not be forced; each circumstance should be evaluated to determine the benefits that a biometric may provide.

Q10: What if my biometric does not work?

On any biometric system, secondary procedures need to be implemented. It is important to remember that biometrics are a component of an overall system architecture, and contingency plans will vary from application to application.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Background

Q: What are the different biometrics modalities and what are their advantages/disadvantages?

Fingerprint

Advantages

- Subjects have multiple fingers
- Easy to use, with some training
- Some systems require little space
- Large amounts of existing data to allow background and/or watchlist checks
- Has proven effective in many large scale systems over years of use
- Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime

Disadvantages

- Public Perceptions
  - Privacy concerns of criminal implications
  - Health or societal concerns with touching a sensor used by countless individuals
- Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust
- An individual’s age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image

Iris

Advantages

- No contact required
- Protected internal organ; less prone to injury
- Believed to be highly stable over lifetime

Disadvantages

- Difficult to capture for some individuals

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea
- Public myths and fears related to “scanning” the eye with a light source
- Acquisition of an iris image requires more training and attentiveness than most biometrics
- Lack of existing data deters ability to use for background or watchlist checks
- Cannot be verified by a human

Face

Advantages

- No contact required
- Commonly available sensors (cameras)
- Large amounts of existing data to allow background and/or watchlist checks
- Easy for humans to verify results

Disadvantages

- Face can be obstructed by hair, glasses, hats, scarves, etc.
- Sensitive to changes in lighting, expression, and pose
- Faces change over time
- Propensity for users to provide poor-quality video images yet to expect accurate results

Hand Geometry

Advantages

- Easy to capture
- Believed to be a highly stable pattern over the adult lifespan

Disadvantages

- Use requires some training
- Not sufficiently distinctive for identification over large databases; usually used for verification of a claimed enrollment identity
- System requires a large amount of physical space

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics

Speaker/Voice

Advantages

- Public acceptance
- No contact required
- Commonly available sensors (telephones, microphones)

Disadvantages

- Difficult to control sensor and channel variances that significantly impact capabilities
- Not sufficiently distinctive for identification over large databases

Others

Many other biometric modalities exist and are in various stages of research or commercialization. Examples include gait (the manner of walking), retina and other vascular pattern recognition, ear structure, odor, and palm prints.

Q: Why are there so many different biometric modalities?

Different applications and environments have different constraints. For instance, adequate fingerprint samples require user cooperation; whereas, a face image can be captured by a surveillance camera. Furthermore, fingerprints are not available for many of the suspects on watchlists. There are also multiple biometric modalities for technical and financial reasons. Many scientists become interested in developing a system based on their own research. Upon a successful implementation, venture capitalist, interested in the implementation of such a system, commercialize a product. Therefore, wide varieties of modalities are being researched and are available on the market.

Q: Can I change my biometrics?

Biological biometrics cannot easily be changed (there have been cases of mutilated or surgically altered fingerprints), but they can be disguised. It may be possible to change a behavioral biometric.

Q: What if identical twins use a biometric device?

Although identical twins may appear the same to the human eye, their biological and behavioral characteristics

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

are usually subtly different. The automated methods implemented in some biometric devices can often identify such differences and differentiate between two seemingly identical twins.

Q: Are biometrics safe to use?

Biometrics are typically passive and designed to be safe to use. Biometric systems usually implement ordinary computing and video technology, such as that encountered in a person's day-to-day activities.

Q: Are biometrics a new idea?

No, methods of recognizing humans have existed for centuries. The most obvious example is the human use of face recognition. Also, handprints were discovered surrounding cave paintings, estimated to be 31,000 years old, and are believed to be the artists' signatures. However, the means for automating such identification is fairly new, dating only to the early 1960s. Automation recognition became possible within the last few decades with the advancement of computer processing capabilities. The individual biometric modalities vary in their stages of maturity. Fingerprint began the transition to automation in the late 1960s, while iris is a little over a decade old. Many methods, such as gait, are still in the research and development stage and are not yet ready for deployment.

Q: Are biometrics intrusive?

This is a subjective question that would be answered differently by various individuals. In general, most biometrics are non-intrusive, requiring only the placement of a finger, a look in the proper direction, or a statement to be said aloud.

Q: Are biometric systems difficult to use?

This question is subjective and depends on each individual. Those users more familiar with electronics technology tend to have fewer issues than those who are not familiar or are skeptical about using technology. From the operational perspective, most people are able to use a biometric system with very little training.

Once I register my biometric, will that registration be good anywhere that specific technology is used?

In general, no. A biometric registered on one system will typically not be valid for another system on which that

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics

biometric might be used. However, if the system on which the biometric was registered is connected to another system, e.g. via a network, then yes, a biometric could also be accepted at the alternate system location.

Q: What is the difference between biometrics and forensics?

While both biometrics and forensics involve human recognition, biometrics is typically applied using automated techniques to the pre-event situation application, such as gaining access to sensitive information or to a secured facility. Forensic applications typically occur after a crime has occurred, and may not use fully automated methods. Forensic methods are often used to assist in the adjudication (legal) process. Forensics usually requires days of processing (versus seconds for biometrics) and are held to much higher accuracy requirements.

Q: What is biometric authentication?

"Biometric authentication" is a generic term for the process of verification. It involves presenting a biometric for query, comparing the presented biometric to a stored template or model, and determining whether the individual has made a legitimate claim.

Q: Do biometric features remain constant over time?

The permanence of biometrics varies between modalities. For instance, fingerprints remain constant over one's lifespan, except for surface wear degrading the prominence and definition of the ridges. Fingerprints are based on physical dermal structures that are defined during fetal development. Temporary or permanent scarring can affect the original fingerprint patterns developed before birth. Aging affects faces more dramatically. Detailed studies of the effects of aging on other modalities have not yet been performed.

Q: What factors contribute to the development of a person's biometric?

A biometric is first affected by the individual's unique genetic makeup. An individual's biometric is also affected by the individual's environment. For example, characteristics such as fingerprints and iris structures are affected by the environmental factors encountered by a fetus in the prenatal environment.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: How do biometric systems determine "matches"?

Biometric systems can be described, albeit in an over-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 templates stored in the database. The results of this comparison are a "match" or a "non-match" and are used for actions such as permitting access, sounding an alarm, etc.

Implementation

Q: What are the common uses of biometrics?

Common examples of biometric use involve controlling access to physical locations (laboratories, buildings, etc.) or logical information (personal computer accounts, secure electronic documents, etc). Biometrics 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.

Q: Where can biometrics be used?

Biometrics can be used in environments where recognition of an individual is required. Applications vary and range from logical access to a personal computer, to physical access of a secure laboratory. They can be used in a variety of collection environments as identification systems. Biometrics are also used for accountability applications, such as recording the biometric identities of individuals boarding an aircraft, signing for a piece of equipment, or recording the chain of evidence. Of course, biometrics perform more reliably in controlled environments, such as offices and laboratories, than in uncontrolled environments, such as outdoors.

Q: Where/How would biometric verification be used?

Verification is used where it is necessary to confirm that an individual is enrolled in a database with the authorizations claimed. In this case, an individual would present a

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

biometric to the system and the system would either verify or not verify that the person is who he or she claimed to be. For example, biometric verification can be used to regulate gaining physical or logical access or for accountability monitoring.

Q: Where/How would biometric identification be used?

Identification is used when the need arises to determine whether or not a person is in a database, absent a claim of identity. In this case, an individual would present his/her biometric to the system and the system would either provide the identity of the person or indicate that the person is not represented in the system. For example, the FBI uses identification methods in its search of fingerprints to determine whether the fingerprint indicates connection to a record of a known person. Another possible application involves using face recognition technology to identify abducted children in a public area or on the Internet.

Q: What are the goals of biometric standards?

Technology standards enable development of integrated, scalable and robust solutions and cut down the cost of development and maintenance of system solutions. Biometric standards have been and are currently being developed on both the national and international levels. Organizations at the national and international levels are focusing on creating a standard set of biometric data interchange definitions, developing standards to promote interoperability between various systems, creating standards for testing biometrics and for testing conformance to biometric standards. According to NIST (NISTIR 6529), standards should be technology neutral and not favor any particular vendor or modality.

Q: What benefits/cost savings will biometrics provide?

The usefulness of biometrics varies from application to application. To determine its true benefit, one must first develop and understand the operational requirements of the application. Biometrics can provide an automated means for identification of an individual or verification of a claimed identity. Before making a decision, one must ensure this task will meet the determined operational needs. Biometrics can potentially provide cost savings through relocating security resources or diminishing the

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

expenses associated with password maintenance, or it could cause extra costs by highlighting problems that were previously missed. The cost benefits vary from application to application as well.

Q: How do I select a biometric technology?

The effectiveness of a biometric technology is dependent on the how and where it is used. Each biometric modality has its own strengths and weaknesses that should be evaluated in relation to the application before implementation. Key decision factors for selecting a biometric technology include evaluating the environment, throughput needs, population size and demographics, ergonomics, interoperability with existing systems, user considerations, etc. For instance, an access control system to a coal mine, where individuals will have very worn and dirty fingerprints, will not be a suitable environment for a fingerprint reader. The careful evaluation of the key decision factors plays a crucial role in the success of the selected technology.

Q: Can everyone be enrolled? If not, then what?

There are some instances when an individual may not have characteristics that are of sufficient quality to enable enrollment in a biometric system. The probability of such instances is small in most application environments, although it is important to have a contingency plan when such failures to enroll occur.

Q: Will biometrics solve all of the security problems?

No, biometrics should be one part of an overall security system implementation plan. A biometric system alone cannot solve a security problem.

Q: How fast does a biometric system work?

This will vary from application to application. It will depend on the hardware and software implemented, user training, the environmental application, and whether human involvement is required in some or all cases to make final decisions. For example, to complete a civil fingerprint background check, the average processing time is approximately 24 hours. On the other hand, implementing fingerprint verification in an airport may be completed in under a second.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: Many access control situations make use of a smart card in addition to a biometric. Why is this necessary?

There are three ways to identify someone: by what they have (a token, e.g. a smart card), by what they know (a pin or password) and by what they are (a biometric). The use of a smart card and a biometric adds a level of security to the system. It incorporates both what they "have" (the smart card) and what they "are" (the biometric). The smart card is often also used to claim an identity for the biometric system to verify. The smart card may contain information (such as cryptographic keys) that may require a biometric for use.

Q: What are the components of a biometric system?

A typical biometric system is comprised of five integrated components. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

Q: What are the processes of a biometric system?

Biometrics systems follow four basic processes: collection, extraction, comparison, and decision. Collection involves using a sensor to capture the biometric traits and convert them to a digital format. Extraction takes the digital data and converts the distinctive features into a compact template. In the comparison step, the biometric system measures the likeness of the template to those in the database. Based on the likeness, the system decides whether or not the submitted biometric matches one of the templates in the database.

Q: Can biometrics be integrated into an existing system?

In general, yes, biometrics can be integrated into existing systems. Like all technologies, however, it is sometimes difficult to integrate biometrics as "retrofits" with existing systems if they weren't designed to accept newer techniques.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: Are biometrics going to affect the time required to do things (e.g. clear airport security, access a secure building)?

Biometric systems may or may not affect the time required depending on the application and the design of both the old and new systems. It is based on the efficiency of the current process. For example: identification at a choke point, if implemented correctly, will not affect the time; DHS' Registered Traveler (RT) program, where individuals have been processed and trusted prior to verification, will decrease the time; and the addition of a system in a location where a system did not previously exist will increase the time.

Q: What factors cause biometric systems to fail?

In addition to common electronics/computer and hardware failures, common biometric issues include poor-quality biometric samples, user confusion, evasion or non-cooperation, noise, inadequate or excessive lighting, dirty sensor, or subject handicaps.

Q: How do you know biometric technology will work as expected?

A properly designed implementation plan involves a series of evaluations, first focusing on algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. If done properly, users will know, to a high degree of accuracy, how the system will perform.

Personal Concerns

Q: How do you know biometric technology is safe (healthy) to use?

Most biometric systems use everyday sensors, such as a digital camera, to obtain the observations of an individual's biometric; other sensors would need to be analyzed. Most stated health concerns are actually similar to those encountered in everyday life (touching a fingerprint sensor is roughly equivalent to touching a doorknob).

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: Can biometrics reveal private information (medical information, drug use, ethnicity, disease detection, etc.)?

Biometric systems cannot detect diseases; however, some of the information gathered using some biometric modalities could potentially be used to detect medical information or drug use. These diagnoses require specialized training, however. The image data from a face recognition system may allude to the individual's ethnicity.

Q: Do biometrics invade an individual's civil liberties and privacy?

Many US Supreme Court findings (e.g. Schmerber v. CA.,384 U.S. 757, 1966; U.S. v Dionisio, 410 U.S. 1, 1973) imply that the use of biometrics does not invade an individual's civil liberties or privacy, although personal viewpoints are subjective and may differ. A well thought through biometric system implementation should be considerate of these issues.

Q: If I provide my biometric, who has access to it (and the information associated with it)?

Access to biometrics stored within the system is a system implementation issue, not a biometrics issue. Each system will be different, and it is recommended that an individual be aware of the use and access to his/her biometrics before providing a biometric to a system.

Q: Can someone steal my biometric(s)?

Although it may be possible to steal one's biometric for use with certain modalities, for example cutting off one's finger or creating a synthetic model of a fingerprint or iris pattern, it is not a practical or realistic concern in most applications. Many vendors are working actively on "liveness" detection mechanisms for determining if a living person is indeed presenting the sample. Although this does not prevent "stealing" of a biometric in all applications, it is an important element in overall system security. In important United States government applications, such as US-VISIT, the biometric is captured in the presence of an immigration officer, who can detect the presence of a forgery. It is important to note that once the system digitizes the biometric data, it faces the same vulnerabilities faced by typical (non-biometric) computer systems.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: What happens if I am enrolled in a fingerprint system and I cut my finger?

Minor scrapes typically do not impact a biometric system. Severe injuries would require a re-enrollment of the healed finger or the enrollment of a different finger. Some biometric systems allow for the enrollment of a secondary sample. For instance, an individual may be able to use his or her left index finger for verification purposes in the event he or she has injured the right index finger.

Performance Statistics

Q: Is there an advantage in combining multiple biometrics?

There is a potential for advancement in some applications if the combination is implemented properly. Combining biometrics incorrectly would result in performance less than that of a single measure.

Q: Is failure to enroll a problem with biometrics?

There are some instances when an individual may not be able to provide an image of sufficient quality to the biometric system. For instance, a fingerprint may not be rolled correctly or there may be dirt on the sensor. Iris technologies are tuned to accept good quality images only. Individual disabilities may exist, such as lacking a finger. The probability of most of these instances is fairly small, but each implementation should have contingency plans in place.

Q: Is the biometric system accuracy dependent on the user?

Yes, to some degree. Some individual users may find using certain modalities more difficult than other users.

Q: How reliable/accurate are biometrics?

Biometric technology is continually improving. The latest government evaluations are available in the Biometrics Catalog, http://www.biometricscatalog.org.

Q: Do biometric matches provide a 100% guarantee?

No technology can provide a 100% guarantee. The key is to determine where the system will be successful and how to implement it correctly for the application. For example, a metal detector must have correct placement and sensitivity

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics

adjustments to work effectively and appropriately; the same is true of a biometric system.

Q: What are the performance metrics (FRR, FAR, TAR, TRR, FTE, etc.)?

Performance metrics require more discussion than this forum allows. Please refer to http://www.biometricscatalog.org/biometrics/biometrics_101.pdf for a detailed description of performance metrics.

Q: How is the accuracy of a biometric system measured?

The accuracy of a biometric system is determined through a series of tests beginning with an assessment of matching algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. If done properly, users will know, to a high degree of accuracy, how the system will perform.

Q: What is a threshold?

A value, predefined by the system administrator or the device producer, which is used to establish the degree of correlation between the biometric provided and the stored template that will result in a match.

Security

Q: Are biometrics more secure than passwords?

In general, security of a system depends on the design of that system and its operational implementation. In general, a properly designed biometric system would be more secure than a properly designed password system because the system is inherently harder to spoof.

Q: Could someone use a replica of the user's biometric to gain unauthorized access to the system?

In rare instances, it may be possible. Although this a question frequently asked, it is more science fiction than a reality. In reality, it is much easier to find alternative weaknesses to a system than to mimic the biometric of a genuine user.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
Executive Office of the President of the United States
National Science and Technology Council

Q: How do performance metrics affect security (e.g. as the FAR decreases, does the security increase)?

There is a trade-off with the relative errors; false acceptance rates generally increasing as false rejection rates decrease. Performance measures, such as a Receiver Operating Characteristics (ROC) curve, highlight the accuracy of a system in a specific instance. This information can be used to maximize the security and convenience based on the needs of the specific application.

Q: Can a biometric be reconstructed from a template?

There have been studies where pseudo-fingerprint images have been reconstructed from the fingerprint template, and face images have been reconstructed from face templates. In these instances, it is essential that specific information about the enrollment process is known.

Q: What is liveness detection?

Liveness detection is used to ensure that only characteristics from a living human being can be enrolled, stored and recognized in a biometric system. Liveness detection can be used to recognize spoof attacks (e.g. submission of a fake biometric sample.)

Q: What happens when a biometric is compromised (stolen)?

Biometrics are one part of an overall system. Actions taken when a system is compromised will vary from system to system.

Q: What is skimming?

The act of obtaining data from an unknowing end user that is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus.

Q: What is eavesdropping?

Surreptitiously obtaining data from an unknowing end user that is performing a legitimate function. An example involves having a hidden sensor co-located with the legitimate sensor.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Modality Specific

Fingerprint

Q: What are slap fingerprints (slaps)?

Slaps are fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card. Slaps are known as four finger simultaneous plain impressions.

Q: How many fingerprints are best?

The number of fingerprints required is application dependent based on the implementation details. While a single fingerprint might prove sufficiently accurate for certain applications, two fingerprints may be required for increased levels of accuracy. In general, ten rolled fingerprints will always have the potential for the highest accuracy, but they take much more time to gather with the current capture technology.

Q: Are fingerprints inherited? Are they more similar between family members than between strangers?

Close relatives may have similar patterns, such as loops, whorls, or arches. This information is typically not used directly for recognition. The minutiae pattern, which is used for recognition, is not inherited or similar; this characteristic even differs between an individual's own fingers and the fingers of identical twins.

Q: Can children's fingerprints be collected?

Yes, in most cases, a child's fingerprints can be collected after the age of one year or so, but the prints may not have the clarity of adult prints. It is not clear whether fingerprints taken from children can be automatically matched to those same individuals later as adults.

Q: What is a "latent fingerprint"?

A latent fingerprint is a fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

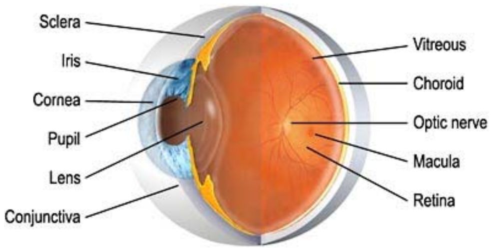
Q: If a latent print is acquired, can it be used to access a biometric system?

Theoretically, yes, some latent prints could potentially be used to gain access to a system implementing biometrics, but it is not a practical or cost-effective approach in most applications. There are easier ways to break into a system. Many systems are implementing liveness detection to prevent attacks such as this from occurring.

Iris/Retina

Q: What is the difference between iris and retina recognition?

Iris recognition uses the unique patterns in the individual's iris, a muscle that is the colored portion on the front of the eye. Retinal recognition uses the unique pattern of blood vessels on an individual's retina at the back of the eye.



[Source: http://www.stlukeseye.com/Anatomy.asp]

Q: Is iris or retina recognition dangerous to the eye?

Iris and retina recognition involve capturing a high quality picture of the iris or retina, using a digital camera. In the acquisition of these images, some form of illumination is necessary. Iris uses near infrared light, which is believed to be safe. Although retina technology is not currently available, previous technology involved the illumination of the retina using infrared and visible light. Literature is inconclusive on the long-term effects of repetitive exposure to this illumination.

Q: Does iris or retina recognition use a laser?

No, neither iris nor retinal recognition makes use of a laser. Both techniques use some form of illumination, but these techniques are not lasers as the term is commonly understood.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: What is the impact of contact lenses on iris recognition systems?

Typically, contacts do not affect the performance of the system, although some color changing and patterned contacts haven proven to be an issue. Also, some issues have occurred in the recognition of individuals wearing hard gas permeable contacts.

Q: Can iris recognition be used for identification purposes?

Yes, it is possible to use iris for identification.

Face

Q: What effects will facial expressions, hairstyle, glasses, hats, makeup, etc. have on face recognition systems?

Minor variances, such as those mentioned, will have a moderate impact on a face recognition system, decreasing its ability to recognize faces. The proposed ISO standard for facial recognition (ISO 19794-5) requires the removal of dark glasses and hats, movement of the hair away from the eyes, and recommends a neutral facial expression. Anything that sufficiently obscures the primary face region will have a negative impact on the recognition system.

Other

Q: What is the difference between speech and speaker recognition?

Speech recognition is the identification of the words being said, and is not a biometric technology. Speaker recognition (sometimes referred to as voice recognition) recognizes the speaker, not the words. Speaker recognition is a biometric technology.

Q: Is speaker recognition language/word independent?

Word independent speaker recognition systems are available and can be used in any language. Whether or not speakers can be recognized if they change languages is the subject of current testing.

Q: What is a behavioral biometric?

A behavioral biometric is one based on an individual's unique actions and is captured over a period of time.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Examples are gait (the way an individual walks), keystroke dynamics, and signature dynamics.

Q: Is DNA a biometric?

There is not universal agreement on this issue. At this point, DNA recognition is not performed by an automated method, and is therefore not considered a biometric; however, it may be at some point in the future.

Q: Is Radio Frequency Identification (RFID) a biometric?

No, RFID is a technology that may be integrated with biometrics. Unlike biometrics, RFID systems are not biologically tied to an individual. RFID is a technology that stores and retrieves data remotely through devices called RFID tags or transponders. These devices use radio frequency (RF) signals to exchange information. They contain antennas that allow them to respond to queries from RFID transceivers. Some examples of RFID tags include sensors in library books, E-PASS Toll Collectors, and building access control cards.

Government Specific

Q: What actions are being taken to ensure stored biometrics data isn’t compromised?

Biometric data is considered sensitive personal information collected by the government and is thus subject to the same laws, regulations, and standards.

Q: What government agencies are researching or working with biometrics?

Many government agencies are working with biometrics. Specifically, the government is implementing the PIV (Personal Identity Verification) Program to issue identity cards with biometrics for all Federal employees and contractors. Federal agencies are also developing and implementing biometrics to meet other operational needs. The National Science and Technology Council (NSTC) is working to coordinate high priority activities within these agencies.

http://www.biometricscatalog.org/NSTCSubcommittee/default.asp

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Q: How accurate are the two fingerprint scans used in US-VISIT?

Actual operational accuracy of the US-VISIT system is sensitive. Data on the basic performance of US-VISIT algorithms is available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7110.pdf. General information regarding the accuracy of commercial fingerprint systems can be found in FpVTE 2003 http://fpvte.nist.gov/.

Q: With regard to domestic and foreign travel, how are biometrics collected at various United States government facilities?

For most foreign visitors to the United States, the DHS's US-VISIT program captures a photograph and two flat fingerprint images that are stored in its IDENT database. Currently, United States citizens are not required to supply biometric data when crossing the borders into or out of the United States.

Q: Are biometrics obtained on everyone that enters or exits the United States?

Biometrics are collected from most foreign visitors entering the United States, but not from United States citizens.

Q: Who has access to the information in government biometric databases?

Personal information access is limited to those individuals who have a "need to know," according to law, to protect United States Government operations.

Q: Which modalities do the Department of "X" use, or plan to use, in the future?

Most departments use a variety of biometric modalities selected based on the needs of the specific applications. These departments are continually re-accessing the uses to determine the method that is in the best interest for maximizing security and prosperity of the country.

Q: Will there be a government-wide standard biometric?

Because no modality is suitable for all applications, there will not be a universal biometric for government use.

Q: Some fingerprint systems use 10 prints, other fingerprint systems use two; some fingerprint systems use rolled

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

fingerprints and other fingerprint systems use flat fingerprints. Why?

> The various collection methods are used to meet a combination of operational needs, current capabilities, cost, and legacy systems. In general, the more quality data one has, the greater precision available; however, more data requires more storage, processing power, etc.

About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees; Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees a number of sub-committees and interagency working groups focused on different aspects of science and technology and working to coordinate the various agencies across the federal government. Additional information is available at www.ostp.gov/nstc.

About the Subcommittee on Biometrics

The NSTC Subcommittee on Biometrics serves as part of the internal deliberative process of the NSTC. Reporting to and

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

directed by the Committee on Homeland & National Security and the Committee on Technology, the Subcommittee:

- Develops and implements multi-agency investment strategies that advance biometric sciences to meet public and private needs;
- Coordinates biometrics-related activities that are of interagency importance;
- Facilitates the inclusions of privacy-protecting principles in biometric system design;
- Ensures a consistent message about biometrics and government initiatives when agencies interact with Congress, the press and the public;
- Strengthen international and public sector partnerships to foster the advancement of biometric technologies.

Additional information on the Subcommittee is available at www.biometrics.gov.

Subcommittee on Biometrics

Co-chair: Duane Blackburn (OSTP)

Co-chair: Chris Miles (DOJ)

Co-chair: Brad Wing (DHS)

Executive Secretary: Kim Shepard (FBI Contractor)

Department Leads

Mr. Jon Atkins (DOS)

Dr. Sankar Basu (NSF)

Mr. Duane Blackburn (EOP)

Ms. Zaida Candelario (Treasury)

Dr. Joseph Guzman (DoD)

Dr. Martin Herman (DOC)

Ms. Usha Karne (SSA)

Dr. Michael King (IC)

Mr. Chris Miles (DOJ)

Mr. David Temoshok (GSA)

Mr. Brad Wing (DHS)

Mr. Jim Zok (DOT)

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Communications ICP Team

Champion: Kimberly Weissman (DHS US-VISIT)

Members & Support Staff:

Mr. Richard Bailey (NSA Contractor)

Mr. Duane Blackburn (OSTP)

Mr. Jeffrey Dunn (NSA)

Ms. Valerie Lively (DHS S&T)

Mr. John Mayer-Splain (DHS US-VISIT Contractor)

Ms. Susan Sexton (FAA)

Ms. Kim Shepard (FBI Contractor)

Mr. Scott Swann (FBI)

Mr. Brad Wing (DHS US-VISIT)

Mr. David Young (FAA)

Mr. Jim Zok (DOT)

Special Acknowledgements

The Communications ICP Team wishes to thank the following external contributors for their assistance in developing this document:

- Kelly Smith, BRTRC, for performing background research and writing the first draft
- Donald Reynolds, Hirotaka Nakasone, Jim Wayman, and the Standards ICP Team for reviewing the document and providing numerous helpful comments

Document Source

This document, and others developed by the NSTC Subcommittee on Biometrics, can be found at www.biometrics.gov.