Global Information Assurance Certification Paper

Biometrics Considerations in High Purity Environments

Laurie A. Behling
GSEC Practical, v.1.4c (August 2004) Option 1
Original submission October 13, 2004

Abstract

As both technology capabilities and security concerns have increased over the last few years, biometrics use is becoming more feasible and desirable in a wide variety of access control applications. However, there are considerations to be made if biometrics technology is to be used successfully within high purity environments. This paper will give an overview of biometrics and various technologies, an overview of high purity environments, and how these environments' special design and requirements must be taken into account when selecting biometrics technology for successful implementation of access control.

Biometrics Overview

What is Biometrics?

Biometrics uses unique personal attributes to identify individuals, either physiological such as fingerprints or retina patterns, or behavioral such as how a person speaks or types.[A] When captured using the appropriate technology, these attributes can then be used as part of authentication, fulfilling the "something you are"[1 B] piece of the three cornerstones of authentication. (The remaining two are "something you know" and "something you have".)[2] For example, companies can assign laptop computers to employees, and the PCs have fingerprint identification systems built-in so that a particular employee's fingerprint ("something you have") will allow access to that laptop to that person but not to anyone else.[C]

The key items to successfully use biometrics for authentication are: the capability of technology to correctly capture and identify individuals, the willingness of people to use the biometric system, and cost. An emerging key item is how easily the attribute can be faked, e.g. someone could gain access to an area by playing a tape recording to a voice, or speaker, recognition system, if the recognition cannot detect whether a live person is speaking or not.

Additionally, when discussing biometrics it is helpful to understand other terminology. How often a system accepts someone as another individual is known as the False Acceptance Rate or FAR, while its opposite of how often a system rejects someone when they are valid is known as the False Failure Rate or FFR.[3] A system that too often allows access to the incorrect person increases the risk of theft, or exposure, of what is being protected. For example, if the goal of using a biometric is to prevent unauthorized access to samples of the Ebola virus being worked on in a biological laboratory (biolab), having a very low FAR is very important. On the other hand, if the goal is to streamline operations, a system that too often denies access to a valid person decreases productivity because of delays caused to genuinely authorized people. Another term is the

[1] SANS, Chapter 9 Access Control p158
[2] SANS, Chapter 7 Defense In Depth p 20
[3] SANS, Chapter 7 Defense In Depth p 20

template, which refers to the pattern of personal attributes that are captured as measurements, rather than as whole images. Templates cannot be stolen and used to impersonate someone else.

There are other considerations about biometrics use, such as legal responsibilities of confidentiality, that need to be resolved before selecting any biometrics system, but these will not be materially discussed in this paper. For more detailed information on these topics and overall biometrics, please see Mr. Cherry's SANS practical.[D]

Types of Biometrics[E]

Physiological:

- Fingerprint measurements of the unique arches, whorls, and loops of the fingerprint are stored digitally, not the entire image. Most fingerprint readers now also have a secondary check for normal body temperature range or pulse.[F] However, even some readers with these secondary checks have been able to be fooled by fake fingers.[G] More discussion on fingerprints as authentication is available in Mr. Spinella's SANS practical.[H]
- Hand geometry provides less detail and few unique features are available for hand measurements compared to the fingerprint, for example, making hand geometry not useful for positive identification. Having a large population increases the likelihood of someone's readings being close enough to someone else's that the two readings are considered matched by the technology, and therefore FAR increases. Changes increasing FFR are also quite likely in hand geometry due to injuries or health conditions.[I] The biggest use of hand geometry is for "punching" time cards, to verify that the correct employee is clocking in. With paper time cards, one employee can punch another employee's time card. If hand geometry is used to create the time stamp for when someone starts working, only the real employee can clock in.[J]
- Iris measurements have far more data points available in the iris than even in the fingerprint. Iris scans are less invasive and less affected by health changes than are retina scans. They are not able to be faked like fingerprints.[K] More detail specifically on iris scanning is available in Ms. Dunker's SANS practical.[L]
- Retina measurements match or exceed that of the iris for uniqueness and accuracy and also like the iris, retinas cannot be faked like fingerprints. However, the scan requires the eye to be quite close to the scanner, reducing people's acceptance, and health changes can increase FFR. Retina scanning is currently the most often used biometric for high risk, high security operations, including military.[M] For more information on retina scanning, please see Mr. Spinella's SANS practical.
- Facial recognition forms a more individual pattern than hand geometry but can suffer from the same FFR due to health and age changes. Facial recognition systems key on areas without hair, so that beards are not likely to increase FFR. Newer systems have also started requiring that the person blink or smile or make some other facial movement, to prove the "face" isn't just a mask. The fact that

current law enforcement uses this technology to look for terrorists in crowds at airports or sports events makes it less likely to be readily acceptable to the general populace if it is seen as being linked primarily with criminals.[N] [O] More detail is available in Mr. Spinella's SANS practical.

- Ear recognition is similar to facial recognition but focuses on the ear, which has more unique measurement opportunities than does the face. Its current driver for investigation is passive identification from a distance, that is, when the person does not know he/she is being identified. It is not a currently available technology and its biggest disadvantage for distance identification is that it is very easy for people to cover their ears with hair or hats.[P]
- Speaker recognition, also known as voice recognition, is accomplished by recognizing the inflections, patterns, and frequencies of a person's speaking voice as matched against that person's stored record to verify that person's identity. It is also known as voice recognition. This is not the same as speech recognition, where the spoken words are interpreted for their meaning. Most speaker recognition systems protect against allowing a recorded voice.[Q] Currently, the most popular use for this biometric is on the telephone, since the hardware is already in place and adding recognition capability is relatively inexpensive.[R] Please see Ms. Meyers' SANS practical for additional specifics on speaker recognition.[S]
- Vascular patterns used in biometrics are those primarily in the hand and are read by an infrared (IR) scanner. Unlike hand geometry, the IR scanner does not require someone to touch the IR scanner for the vein pattern to be read. This is an advantage for people who have sanitary concerns about everyone touching the same device for their fingerprint or hand geometry reading. The pattern of the veins is currently believed to be quite complicated and intricate, making it difficult to try to falsify. This technology does not have the disadvantage of hand geometry technology that requires no cuts, bandages, or other external differences from the original hand measurement.[T]
- DNA recognition is currently used primarily in court cases rather than commercial applications. With accurate testing, it is perfectly accurate though it could be fooled through substitution i.e. someone's hair is submitted for identifying someone else.[U]

Behavioral:

- Signature recognition is based on the rhythm in how a name is written, with jabs or smoothly for example, not the picture of signature itself. The variations in signatures leads this technology to have a higher FFR than FAR, so that while it is difficult for someone else to fake another's signature, someone can more easily fail at their own signature. While not in much use at the present time, signature recognition is expected to become more popular as verification associated with tasks that already require a signature such as contracts.[V]
- Keystroke dynamics is based on the rhythm and timing of how someone types on a computer keyboard. It is not unique enough by itself to form the sole means of identification. However, when combined with a typed password

("something you know"[4]), the resultant "hardened password"[5] is effective in protecting against password cracking attacks.[W] There may be ergonomic concerns about repetitive trauma if long sections of text must be typed often for verification.

- Step pattern, or gait recognition, has more than one analysis methodology including radar and walking over force plates. Both also include video analysis. The radar technique is aimed at identifying people at a distance of up to 500 feet away, with the goal of identifying terrorists as they approach a protected location. The force plate technique requires special flooring and sensors in the authentication vicinity, which may have more usefulness in access control into an area rather than access control to, say, computer systems within the area. Both methods require a half dozen or more steps to gather enough data for recognition.[X Y]

A Biometrics Comparison Chart shown in Table -1 from the National Center for State Courts web site gives a visual summary for comparing several biometrics. While the 16 aspects given in the table below are important for any biometric use, the environment in which the biometric is to be used must also be considered in order for the deployment to be successful. Biometric authentication implementation on a scale from a few dozen up to thousands of employees is challenging enough in itself without inadvertently fighting against the surroundings as well.

[4] SANS, Book 2- Defense In Depth p20
[5] Monrose, p. 1.

Table 1 – Biometrics Comparison Chart[6]

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	✓	✓	◎◎◎◎	▶▶▶	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	✓	✗	◎◎◎	▶▶	No data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	✓	✗	◎◎◎	▶▶	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	✓	✗	◎◎	▶	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	✓	✓	◎◎◎◎	▶▶▶	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	✓	✓	◎◎◎◎	▶▶▶	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	✓	✗	◎◎	▶	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	✓	✗	◎	▶	no data	hand injury, tiredness	Difficult	Easy
DNA	✓	✓	◎◎◎◎	▶▶▶	no data	none	Ext. Diff.	Ext. Diff.

Aspect descriptions:

Verify	Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be.
ID	Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many people to see which person the user is.
Accuracy	How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.
Reliability	How dependable the Biometric is for recognition purposes.
Error Rate	This is calculated as the crossing point when graphed of false positives and false negatives created using this Biometric.
Errors	Typical causes of errors for this Biometric.
False Pos.	How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else).
False Neg.	How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself).

[6] http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html

Table 1 – Biometric Comparison Chart (con't)

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	▶▶▶	▶▶▶	▶▶	Somewhat	▶▶▶	✓	Special, cheap	Yes
Facial Recognition	▶▶	▶▶	▶▶	Non	▶▶	✓	Common, cheap	?
Hand Geometry	▶▶	▶▶	▶▶	Non	▶▶▶	✗	Special, mid-price	?
Speaker Recognition	▶▶	▶▶	▶▶▶	Non	▶▶▶	✓	Common, cheap	?
Iris Scan	▶▶▶	▶▶▶	▶▶	Non	▶▶	✗	Special, expensive	?
Retinal Scan	▶▶▶	▶▶▶	▶▶	Very	▶	✗	Special, expensive	?
Signature Recognition	▶▶	▶▶	▶▶	Non	▶▶▶	✓	Special, mid-price	?
Keystroke Recognition	▶▶	▶	▶▶▶	Non	▶▶▶	✓	Common, cheap	?
DNA	▶▶▶	▶▶▶	▶	Extremely	▶	✗	Special, expensive	Yes

Security Level	The highest level of security that this Biometric is capable of working at.
Long-term Stability	How well this Biometric continues to work without data updates over long periods of time.
User Acceptance	How willing the public is to use this Biometric.
Intrusiveness	How much the Biometric is considered to invade one's privacy or require interaction by the user.
Ease of Use	How easy this Biometric is for both the user and the personnel involved.
Low Cost	Whether or not there is a low-cost option for this Biometric to be used.
Hardware	Type and cost of hardware required to use this Biometric.
Standards	Whether or not standards exist for this Biometric.

High Purity Environment Overview

What are High Purity Environments (HPE)[z]

An example of an HPE, and also the first type of cleanroom ever used, is a hospital operating room. The two broad classifications of HPE reviewed in this paper are cleanrooms and biolabs. Cleanroom environments are, as the name implies, very dust-free as the items made there are extremely sensitive to particles during the manufacturing process. For example, semiconductor chip transistors are now smaller than many of the dirt particles which, if the dirt landed in the wrong place, could make the chip unusable.

Another cleanroom example is pharmaceutical manufacturing. The stakes of product contamination are much higher than an unusable computer chip, since contaminated products become unsafe medicines. Therefore, pharmaceutical manufacturing is very concerned with contamination of product and is highly regulated by the U.S. Food and Drug Administration (FDA). Even some foreign companies follow FDA regulations to be able to sell their products in the U.S. Microbiological monitoring occurs in addition to the typical cleanroom particulate monitoring. Critical areas, as defined by the FDA where sterilized product is exposed to the environment, must be kept at class 100. Control areas, again defined by the FDA as where non-sterile containers or product portions are handled, must be kept at class 100,000.[7] [AA] Cleanroom classes are defined by the number of particles allowed per cubic foot of air. The lower the class number is, the fewer particles are allowed in the air.

Biolab environments are where disease research takes place and emphasis is on containment of the products as well as on contamination potential to employees.

Cleanroom classification levels

More precisely, a cleanroom is

> An area in which the concentration of airborne particles is controlled, and which is constructed and used in a manner to minimise the introduction, generation, and retention of particles inside the room and in which other relevant parameters, e.g. temperature, humidity, and pressure, are controlled as necessary.[8] [BB]

Particle control is continually pursued through a variety of means, each contributing to the overall level of the cleanroom such as:

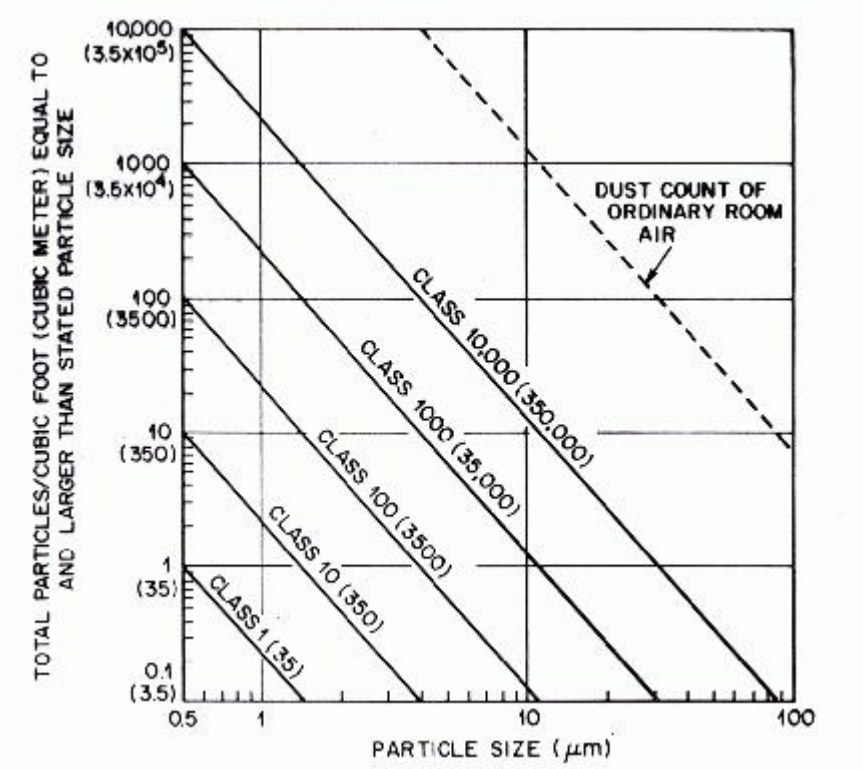
- unidirectional airflow (e.g. from ceiling to floor) to keep particles from settling
- special material air filters to catch particles before getting into the cleanroom
- air exchanges of up to several room-exchanges per minute to dilute particles
- minienvironments of smaller spaces to contain product which are easier to keep particle-free
- personal protective equipment to contain human body particles
- materials for furniture and equipment are all non-particle shedding[9]

In addition to design and construction considerations, particle control is also pursued through people's behavior during movement within the HPE. A sitting person, such as typing on a keyboard, generates about 100,000 particles per minute (PPM). A standing person with limited movements, such as moving product on a workbench, generates about 1 million PPM. A walking person generates about 5 million PPM.[CC]

---

[7] http://www.s2c2.co.uk/docs/classificationofcleanrooms2004.pdf p.7
[8] http://www.dycem-cc.com/basics.html
[9] Whyte, ed. P. 17

The following Graph-1[10] [DD] shows particle size vs. particles per cubic foot for various cleanroom classes:



Personal Protective Equipment (PPE) required for cleanrooms includes a smock or coat, a haircover or hood, shoecovers, and gloves. For cleanrooms that allow the most particles, this is all that is required to maintain the class rating. As the class of cleanroom becomes more stringent, add a facemask, special boots over the shoecovers, and coveralls instead of a smock or coat.[EE]

Per the United States Government Department of Labor Occupational Health and Safety Administration (OSHA), "Personal protective equipment, or PPE, is designed to protect employees from serious workplace injuries or illnesses resulting from contact with chemical, radiological, physical, electrical, mechanical, or other workplace hazards."[11] [FF] Thus, safety glasses are required not for the purpose of keeping particles out of the cleanroom but generally as part of overall safety. Additional safety equipment, such as acid-proof face shields, gloves, and aprons, is also required by OSHA when working with acids, for example.

Biological laboratories classification levels[GG]

Biolabs perform research with disease-causing agents of varying hazard levels 1 through 4 as defined by the National Institutes of Health. The environments in

[10] http://www.ee.byu.edu/cleanroom/particlecount.phtml
[11] http://www.osha.gov/OshDoc/data_General_Facts/ppe-factsheet.pdf

the biolabs are designed to protect the outside atmosphere from contamination by the diseases under research, and the PPE protects the people working inside from disease.

1. Biosafety Level 1 (BSL-1): Agents investigated at this level do not generally cause diseases in healthy adults. An example is *E. coli*.[12] The facility can have inward air pressure but does not have to. PPE consists of a lab coat, gloves, and possibly eye and face protection.

2. Biosafety Level 2 (BSL-2): Agents examined at this level are considered intermediately dangerous and include measles and hepatitis B.[13] The facility must meet all of the BSL-1 requirements, and the added requirements for BSL-2 are that the room must be lockable and have a BSL-2 biohazard sign.[HH] PPE is the same as BSL-1, and in addition, procedural precautions to avoid contaminated sharps.

3. Biosafety Level 3 (BSL-3): Agents studied are dangerous and potentially lethal when airborne, including *M. tuberculosis.*[14] The facility must meet all of the BSL-1 and BSL-2 requirements, and the added requirements for BSL-3 are that the room must be isolated or must be a completely separate building, must have a double-door entry, and must have inward air pressure flow. PPE includes the same equipment for BSL-1 and BSL-2, and in addition, respirators.

4. Biosafety Level 4 (BSL-4): Agents researched are extremely life threatening such as Ebola virus. The facility must meet all of the BSL-1, BSL-2, and BSL-3 requirements, and the added requirements for BSL-4 are that there must be interlocked doors and dedicated air systems. PPE includes the same equipment as BSL-1, BSL-2, and BSL-3, and in addition, can be an entire body suit with its own, positive-flow air supply, or researchers step into upper body half-suits, which are permanently attached to airtight cabinets containing the disease agents. [15]

Personal Protective Equipment used in HPE[II]

There are always two reasons to use PPE in HPE. In cleanrooms, employees first use PPE to protect the delicate human bodies from some of the potential hazards in the manufacturing process, and secondly, protect the delicate products from particles generated by human bodies. In biolabs, employees use PPE to protect themselves from the diseases they research, and secondly, protect their disease samples from contamination. Since PPE can cover a great deal of the human body, the next section compares PPE requirements along with biometric technology requirements.

- Fingerprints are currently not able to be read through gloves, though reader manufacturers are working toward machines that are capable of reading fingerprints through latex gloves. Most areas of cleanrooms that do not require extra gloves such as for acid work for example, would be able to use this new

[12] Richmond, p. 9
[13] Richmond, p.23
[14] Richmond, p. 42
[15] Badkhen, p. 5

type of reader.[JJ] It is not clear whether each person would need two measurement sets, one with gloves and one without, nor is it clear that the materials in the reading device would be acceptable in an HPE. With today's technology, fingerprints are not usable for authentication within an HPE.

- Hand geometry is possible to read through gloves, though this technology may have increased FAR as readings between people may become closer (with a large enough enrolled population) with the feature-smoothing effects of gloves. Installation room for the readers may also be an issue in the HPE. Hand geometry may be usable for authentication within an HPE. This technology would have to be tested with HPE PPE to determine if its FAR would be acceptable in the particular situation.
- Iris scans are able to perform through glasses, so the safety glasses and BSL- 4 full body suits with face plates are no issue with this technology. (Gunsch, p.7) Since some iris scan products can be affected by lighting, the varying lighting levels required by some HPE products in the manufacturing process need to be taken into account. However, there is at least one iris scan product, PrivateID, which is little affected by light levels.[KK] Iris scanning is usable for authentication within an HPE.
- Retina scans do not work through glasses. Due to safety glasses being required or at least recommended at every level of cleanroom and biolab classification, retina scans cannot be used for identification within HPE without violating safety procedures and so is unusable. Also, retina scans are dependent on good lighting, more so than iris scans. Retina scanning is not usable for authentication within an HPE.
- Facial recognition is at a severe disadvantage in an HPE. Despite pinpointing the portion of the face least changing due to facial hair, face masks that cover the mouth, cheeks, and nose, and hoods that cover the forehead leave little except the eyes exposed for measurement. Since facial recognition also depends heavily on good lighting like retinal scans, the varying lighting levels required in the manufacturing process by some HPE products would also cause a high FFR. Facial recognition is not usable for authentication within an HPE.
- Ear recognition has an even worse disadvantage in an HPE than does facial recognition. Since almost all levels of HPE require the hair to be covered, the ears would be covered as well and thus are unavailable for scanning. Ear recognition is not usable for authentication within an HPE.
- Speaker recognition requires a quiet environment to discern voice characteristics. Most products are able to verify speakers even with a mask, but since a large weapon against particulate contamination in HPE is continual airflow, such an environment is likely to be too loud to have an acceptable FFR. If speaker recognition is to be used outside of the HPE as well, two voice prints will be needed: one with the mask for use only in the HPE and one without the mask for use only outside the HPE. Speaker recognition may be usable for authentication within an HPE. This technology would have to be tested with HPE PPE to determine if its FFR would be acceptable to the particular situation. For example, measure the decibels in the HPE and compare against the requirements for the desired speaker recognition technology.

- Vascular patterns in the hand do not suffer the same disadvantages of fingerprints and hand geometry because they are read by an infrared scanner. The infrared scanner is not affected by gloves just as it is not affected by bandages on the hand. As with hand geometry, installation room for the readers may be an issue in the HPE.[LL] Vascular hand pattern scanning is usable for authentication within an HPE.
- DNA recognition is dependent on human body particles and so is unsuitable for an HPE using the current technology. DNA recognition is not usable for authentication within an HPE.
- Signature recognition itself is not immediately ruled out in an HPE, though dual recognition as for speaker recognition would likely be needed due to gloves. Speaker recognition may be usable for authentication within an HPE. The devices used for the signature would have to be carefully tested for particle dispersion to be sure they are acceptable in a particular situation.
- Keystroke dynamics would not have signature recognition's possible device disadvantage, since keyboards are widely used in HPEs. It may require dual templates, though, if typing with gloves shows an increase in the FFR. Keystroke dynamics is usable for authentication within an HPE.
- Step pattern, or gait, recognition has the immediate drawback of requiring extra space in the HPE. An even bigger disadvantage is that it requires extra movement where every movement causes particle dispersion in cleanrooms. It also may not be recommended for BSL-4 body suits and certainly is not usable for BSL-4 half-suit safety cabinets. Step pattern recognition is not usable for authentication within an HPE.

Conclusions

HPE Biometric contenders rated against key success criteria

How do the usable technologies also meet the key biometric criteria previously discussed?

- Hand geometry is most reliable as a verification tool, not an identification tool, and will likely have higher FFR when used with PPE. It has adequate user acceptance but still has a higher cost than the behavioral technologies which also provide a verification level of authentication. Without pulse or temperature tests by the reading device, it is possible to be faked.
- Iris scan has no issues with any HPE PPE, and using the previously mentioned PrivateID product, nor are there environmental issues. It is within the top 2-3 most accurate and lowest error technologies (retina and DNA), is more acceptable to users than those, and cannot be faked. However, again along with retina and DNA testing, it is one of the most expensive biometric technologies.
- Speaker recognition is best used as verification, not identification, and there is the difficulty of managing and tracking two measurements for each employee. That is, if the HPE is quiet enough for speaker recognition to have an acceptable FFR. It has a high overall error rate and may be faked entirely if the technology cannot differentiate a tape recording from a live voice. It does have good user acceptance and is inexpensive if used over existing telephones.

- Vascular patterns in the hand read by IR are able to be used as absolute identification of the individual, not just verification against someone's known template. The technology is too new to have wide user experience or acceptance in the field but should be more appealing to users than hand geometry since no touch is required. It is considered extremely difficult to fake. Cost is moderately high, above hand geometry but below iris scans.[MM]
- Signature recognition is most valid for verification, not identification. It would add the difficulty of managing and tracking two measurements for each employee and that is only if the devices used for the signature are approved for HPE use. It has moderate user acceptance and is low cost. It is difficult to fake in that even genuine signers are occasionally rejected falsely so imposters are rejected at an even higher rate.
- Keystroke dynamics, as with signature recognition, has the drawback of being a behavioral biometric, so it is more suited to verify someone *along with* another authentication item rather than providing identification. It has good user acceptance, and is inexpensive to implement in locations already fitted with keyboards.

Summary

Outdoor use, where the weather and other uncontrolled external factors must be contended with, is at one end of the spectrum of environmental extremes for biometrics technologies. At the other end are the HPEs that have been discussed in this paper. While a wide variety of biometrics may be planned or already used to authenticate someone to *enter* an HPE, the use of the same biometric to authenticate the same person when they are *inside* an HPE may require a dual enrollment, may not be possible at all due to HPE requirements, or may have such an increase in FFR as to be useless for authentication purposes. From the least preferred technology to most preferred technology:

6. Speaker recognition is sixth as it will most likely not be usable in HPE, is verification only, and has dubious accuracy. However, its excellent user acceptance and low cost may somehow fit a particular HPE situation and may be worth testing.
5. Signature recognition is fifth since its technology may have a particulate issue. It is a verification technology and has a high FFR.
4. Hand geometry is fourth as a verification technology and an increased likelihood of an unacceptable FAR due to gloves.
3. Keystroke dynamics is third as another verification technology. It has good user acceptance and costs. It needs extra testing to determine if gloved measurements must be taken along with ungloved measurements.
2. Vascular patterns infrared recognition in the hand is ranked second as next most accurate for identification and having no conflict with HPE PPE. However it is too new yet to have data on user acceptance and what the costs really are in deployment.
1. In terms of meeting the most key biometric capabilities, as well as HPE and PPE requirements, the preferred biometric for authentication is iris scanning. Iris

scanning has the least conflict with a high purity environment and required protective equipment. It meets the key criterion of being one of the most reliable and accurate identification biometrics available, and it is available with today's technologies and ready for implementation. It is accepted by users moderately well. Its cost is its largest disadvantage, though as web cams and PCs decrease in cost, so do the costs of iris scanning.[NN]

References

[A] Cole, Eric et al. SANS Security Essentials & the CISSP 10 Domains. Version 2.2 Book 2 Defense In Depth. USA:SANS Institute Chapter 9 "Access Control and Password Management"

[B] Cole, Eric et al. SANS Security Essentials & the CISSP 10 Domains. Version 2.2 Book 2 Defense In Depth. USA:SANS Institute Chapter 7 "Defense In Depth"

[C] Poletti, Therese. "ThinkPad to have fingerprint reader" 11 October 2004. http://www.mercurynews.com/mld/mercurynews/business/technology/personal_technology/9889956.htm?1c (10/12/2004)

[D] Cherry, Kyle. "Biometrics: An In Depth Examination" (SANS reading room) November 2003. http://www.sans.org/rr/papers/index.php?id=1329 (10/03/2004)

[E] National Center for State Courts (NCSC) http://ctl.ncsc.dni.us/biomet%20web/BMIndividuals.html (10/03/2004)

[F] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html (10/02/2004)

[G] Matsumoto, Tsutomo et al. "Impact of Artificial "Gummy" Fingers on Fingerprint Systems." Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002. http://cryptome.org/gummy.htm

[H] Spinella, Edmund. "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning" (SANS reading room), 28 May 2003 http://www.sans.org/rr/papers/index.php?id=1177 (10/02/2004)

[I] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMHand.html (10/03/2004)

[J] http://www.biometricgroup.com/reports/public/reports/hand-scan_applications.html (10/02/2004)

[K] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMIris.html (10/02/2004)

[L] Dunker, Mary. "Don't Blink: Iris Recognition for Biometric Identification" (SANS reading room), 20 November 2003. http://www.sans.org/rr/papers/index.php?id=1341 (10/02/2004)

[M] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html (10/03/2004)

[N] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html (10/03/2004)

[O] Bonsor, Kevin. "How Facial Recognition Systems Work." http://www.howstuffworks.com/facial-recognition.htm (10/02/2004)

[P] Burge, Mark. Burger, Wilhelm. "Ear Biometrics" http://www.computing.armstrong.edu/FacNStaff/burge/pdf/burge-burger-us.pdf (10/03/2004)

[Q] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMSpeaker.html (10/04/2004)

[R] http://www.biometricgroup.com/reports/public/reports/voice-scan_strengths_weaknesses.html (10/04/2004)

[S] Meyers, Lisa. "An Exploration of Voice Biometrics." (SANS reading room), 19 April 2004. http://www.sans.org/rr/papers/index.php?id=1436 (10/02/2004)

[T] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMVascular.html (10/05/2004)

[U] Meeker-O'Connell, Ann. "How DNA Evidence Works" http://www.howstuffworks.com/dna-evidence.htm (10/03/2004)

[V] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMSignature.html (10/03/2004)

[W] Monrose, Fabian. Reiter, Michael K. Wetzel, Susanne. "Password Hardening Based on Keystroke Dynamics." http://www.bell-labs.com/user/fabian/papers/acm.ccs6.pdf (10/05/2004)
[X] Sanders, Jane. "Walk the Walk: Gait Recognition Technology Could Identify Humans at a Distance." Georgia Tech Research News. Research News & Publications Office, Georgia Institute of Technology. 11 October 2002. http://gtresearchnews.gatech.edu/newsrelease/GAIT.htm (10/07/2004)
[Y] Cattin, Philippe C. Zlatnik, Daniel. Borer, Ruedi. "Biometric System using Human Gait" Institute of Robotics, Swiss Federal Institute of Technology. Http://people.ee.ethz.ch/~pcattin/papers/M2VIP_2001.pdf (10/06/2004)
[Z] Whyte, W. ed. Cleanroom Design. Chippenham: John Wiley & Sons Ltd, 1999.
[AA] http://www.s2c2.co.uk/docs/classificationofcleanrooms2004.pdf (10/07/2004)
[BB] http://www.dycem-cc.com/basics.html (10/07/2004)
[CC] Whyte, W. Cleanroom Technology – Design, Testing, and Operation. Chippenham: John Wiley & Sons Ltd, 2001.
[DD] http://www.ee.byu.edu/cleanroom/particlecount.phtml (10/6/2004)
[EE] http://www.esd.tv/pdf/cleanroom_environments.pdf August 2001 (10/09/2004)
[FF] http://www.osha.gov/OshDoc/data_General_Facts/ppe-factsheet.pdf (10/08/2004)
[GG] Richmond, Jonathan Y.McKinney, R.W. "Biosafety in Microbiological and Biomedical Laboratories." 3rd edition. 5th National Symposium on Biosafety. http://www.cdc.gov/od/ohs/symp5/jyrtext.htm (10/07/2004)
[HH] Badkhen, Anna. "Fear follows plan to build more deadly-disease labs" San Francisco Chronicle 22 August 2004 http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/08/22/MNGEV8CDPT1.DTL (09/30/2004)
[II] NCSC http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html (10/02/2004)
[JJ] Gunsch, Trace. Silk, Greg. "Biometrics Technology" U.S.Army Information Systems Engineering Command, Technology integration Center August 2000. http://www.hqisec.army.mil/TIC/documents/2000/00-035.doc (10/03/2004)
[KK] Soto, Carlos A. "Look me in the eye—or in the face" Government computer News vol. 21 no.9. 29 April 2002. http://www.gcn.com/21_9/reviews/18488-1.html (10/10/2004)
[LL] Quam, Dr. William. "Hand Scanner" http://www.eml.doe.gov/hsrd/hsr03/STL.htm#STL-01-1310 (10/07/2004)
[MM] Shen, Michelle. "The 'People' Element in Biometrics and Physical Access Control". 14 April, 2003 http://www.biometritech.com/features/shen041403.htm (10/10/2004)
[NN] Perrin, Richard A. "Biometrics technology adds innovation to healthcare organization security systems" Healthcare Financial Management. March 2002. http://www.findarticles.com/p/articles/mi_m3257/is_3_56/ai_83762243 (10/11/2004)