Global Information Assurance Certification Paper

The Future Challenges of Biometrics

Lee Eng Chuah
GSEC Practical Assignment (Version 1.4) Option 1
July 25, 2002

Abstract

Current schemes of authentication comprise of three main elements - "something you know" (for example password and personal information), "something you have" (for example token and identity card) and "something you are" (for example biometrics). A large number of cases shows that "something you know" tends to be forgotten or shared out, and "something you have" tends to get lost or being stolen. Therefore, biometrics is emerging as the preferred solution for authentication and identification because it cannot be forgotten or lost. However, are these features truly unbeatable? How secure are they? What is the impact of this technology to the society?

This paper will examine the two main challenges faced by biometrics, namely the technological and social challenges. The effectiveness of biometrics as an authentication and identification tool in replacement of passwords and tokens will be explored based on the vulnerabilities and ease-of-use of the technology. It is crucial that more research focus on the design of biometric system, both the hardware and the software, to eliminate its vulnerabilities and enhance its usefulness. In addition, appropriate policies and regulations need to be in place to build up confidence amongst the public to use biometrics with comfort. Finally, the paper briefly describes several emerging biometric applications that are worthy of attention because of the potential benefits and implications they hold for society.

Biometrics, the Authentication and Identification Tool

The Uniqueness

As the history of mankind progresses, we observe the increasing need to identify or authenticate people whom we are dealing with in our daily life. Methods of identification that started with appearances and names became more sophisticated as time goes on whereby people associate more and more data such as birth certificate, codes, knowledge about family and token to a man to label him/her as the only unique person in the world. The primary reason is just to gain complete confidence that communication is directed to the right person. Things get even more complicated when computers come in between and the two parties at each end of the communication channel have to rely fully on a well-established and reliable authentication scheme to build their trust of communication.

Biometrics is the automated use of physiological or behavioral characteristics of human being to positively identify the person (IBG, 2002). The physiological features are those of human body parts such as fingerprint, facial appearance, and hand's shape while behavioral features refer to those characteristics resulting from the action of a human being such as voice and signature. Biometrics is generally associated with automated process or computerized system where the whole process of capturing, analyzing, comparing and making decision works with bits-and-bytes information. Therefore, although people have used methods such as facial or voice recognition for long, the techniques used then are more based on subjective and emotional judgment. Another distinctive feature of the biometric technology is the existence of templates that are being used to compare with the subject being identified or authenticated.

Through investigation and experiments, scientists claim that biometric features are unique to every single person, that essentially no two individuals share the same biometric data. The uniqueness of biometrics is due to its infinite number of possible combinations of a large pool of parameters, which greatly outnumbers the whole population of human beings in the world.

Seemingly, every substance or object can be represented or interpreted in digital information, the "0"s and "1"s. That explains why the biological form of human body could be translated and manipulated with the use of computers for authentication and identification purposes.

The Technologies

Biometric technologies widely in use today include finger scanning, facial recognition, iris scanning, retina scanning, hand-geometry scanning, signature scanning and voice scanning. Other types of biometrics that are still in the exploratory stage are vein scanning, DNA, human scent, etc. It is so certain that more biometric features that can be used as human identifiers will be discovered in the future.

Identification is the process of recognizing a person and the outcome usually relates names, gender, address and other personal particulars to that person. An example of this would be the recognition of a victim in an accident based on the driving license carried by the victim. It is sometimes termed as 1-N matching as the subject to be identified is usually compared to a huge number of existing templates whereby the identity of each has been established (IBG, 2002).

Authentication on the other hand is the act of proving that the person is really who he/she claims to be, for example when a person types a password to gain access to the computer and it is expected that he/she who knows the password is the person holding the user account. This kind of system is also known as 1-1 matching system (IBG, 2002).

The Process

Biometric authentication or identification involves multiple stages: enrollment, submission, comparison and decision-making.

The enrollment stage is the first time a new user submits his/her biometric sample through biometric acquisition device. The sample acquired will then be processed (for example features extraction and image enlargement) and turned into a template that is then stored in either a central database or some token form such as smart cards.

During the submission stage, which is the actual authentication or identification stage, a user who desires to access the protected computer systems or secured facilities submits the required biometric sample to the system, which will then compare the submitted sample with the templates created at the enrollment stage.

Lastly, a decision will be made by the system based on the degree of correlation between the template/templates and the submitted sample. The decision could be “access granted” or “access denied” as in an authentication system or in the case of an identification system, the name or profile of the subject being scanned. The administrator of the system sets the decisive point between a “yes” and “no” by configuring the desired percentages of match between the templates and the submitted sample.

The Applications

The implementation of biometric system is possible for all areas that are now using either “something you know” or “something you have” for authentication or identification purposes. Biometric systems serve major security functions such as physical access control, computer and network access, e-commerce applications, time and attendance system, detection of criminal suspects in a crowd and user identification system in the public service departments to avoid enrollment of the same user under multiple identities.

Technological Challenges: Security and Reliability

Overview

The call for an information security system stems from the need to protect the state of confidentiality, integrity, authorization and non-repudiation of the information. All of these can be achieved by ensuring that only the right person has access to the information. The use of password and/or smart cards to deliver the above functions is found to be insufficient in the face of increasingly cunning

techniques of hacking, system intrusion and forgery. Besides, too many cases indicate that simple password tends to be compromised and complex password is easily forgotten, while smart cards can get stolen or lost. This has indeed added to the cost of maintaining the system. Consequently, the limelight was shone on biometrics, a technology that is regarded as the best solution. In addition to the functionality of protecting the information, it can also be used to identify the person in question in the event of crime, disaster or fraudulence. The question now is how well can biometric technology address the expectations of the community in safeguarding information?

The characteristics of biometrics such as fingerprint or iris pattern are highly complicated and their variations are well beyond men's knowledge. Logically, we can really count on them as the unique identifier representing a person. However, in reality, these complex biometric features are to be manipulated and analyzed by computer systems, which consist of hardware and software. Therefore, biometric application is as secure and reliable as the hardware, software and the transmission media or the algorithms used to process the biometric data.

Accuracy

Two well accepted metrics that measure the performance of biometrics are False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR refers to the rate at which access is granted by error to the person who should not have the rights to access the system; FRR is the probability that the biometric system falsely deny access to users who have enrolled in the system (Cardwell, 2001). The use of such metrics is due to the interesting fact that the same biometric feature of a user can never generate two identical templates.

Environmental factors like humidity and light intensity, human aging process and random factors such as variation of posture, area of exposure of the biometrics, variation of pressure applied by the hand, and inconsistent performance of the hardware used render the generation of any two identical templates impossible.

The occurrence of either false rejection or false acceptance is accounted for by the fact that all current biometric systems require users to standardize their process of submitting biometric samples. That is to say, the sample must be taken under conditions as close as possible to the conditions during the enrollment process (Soto, 2002). In reality, this is not always possible all the time. For example, a voice recognition system maybe sensitive to the ambient sounds such as the sound of air-conditioning system whereby the users have to turn on the air-conditioning system each time he submits the voice sample, if the sound of the air-conditioning system was captured during the enrollment process.

A finger scanning system might fail if the fingers scanned are cold; pressure of placement is different than those during the enrollment process or there is a cut

on the finger. More factors have been found to fail biometric verification such as wearing of glasses, colored contact lenses, lighting intensity and others. In addition to these physical or environmental changes, a user may also not be able to recall how he/she submit his biometric samples if the last verification/enrollment process was too long ago.

Therefore, there could never be a 100% match or accuracy of a biometric system (IBG, 2002). A biometric system can only make a decision to accept or reject the authorization of a person based on a threshold value set by the administrator of the system. If the percentage of matching between the template submitted and the template stored is above the threshold value, then the person is recognized by the system as the same person who was enrolled before, thus he/she is granted access and vice versa. Knowing the fact, a person can artificially create a biometric data set that is not necessarily 100% exact to spoof a system, as long as the percentage of similarity is higher than the threshold value set on the biometric system.

Vulnerabilities

A recent report reveals that the facial recognition technology tested at the Palm Beach International Airport failed to correctly identify airport employees 53 percent of the time over a month-long period of test (Scheeres, 2002). The vendor of the product argued that the poor outcome was caused by improper control of the application, for example incorrect lighting. Hence, the design issue should be given more consideration in the light of random environmental factors to minimize the error rate.

The algorithms used by different vendors for different biometric product are also based on certain mechanisms, which can be fooled. There are three possible ways to trick a biometric system. The first one is to use artificially created biometric features such as fake fingers. The second way is to trick the system by playing back the biometric data captured in the previous authentication process and the last approach is the theft of the biometric data after getting into the database that stores the biometric templates (Thalheim, Krissler and Ziegler, 2002).

Recently, there was this astounding news of how fingerprint recognition devices were fooled by very low-end materials and techniques (Leyden, 2002). Tsutomo Matsumoto, a Japanese cryptographer created a fake finger using gelatin and a plastic mould. The fingerprints of the fake finger were then created using latent fingerprints collected from a glass and etched on a photosensitive printed-circuit board, which are available from many electronic hobby shops. It was found that this cheap creation did an incredible job in fooling the fingerprint recognition devices to believe that the finger scanned indeed came from its owner.

That is only one of the many examples of people succeeding in tricking a biometric authentication system. Many tests have been conducted and more are under way to evaluate the performance of biometric systems. Thus far, none of the existing biometric system was found to be foolproof.

To outwit a fingerprint scanner, one can use a fake finger (as done by Tsutomo). Although many vendors have claimed that their product can differentiate between a dead and a live finger, the numerous cases of system being broken in via fake fingers only serves to prove that this type of system is still susceptible to attacks. The reason being that each system uses a particular algorithm that collects specific accompanying data set such as pressure, humidity and temperature of the finger. As soon as one gets to know of how the algorithm works and the preferred value of each variables, impersonation is as easy as getting the correct combination of data value.

Apart from that, reactivation of latent fingerprints has also shown very high success rate in tricking the finger scanning system. The latent fingerprints left on the sensor's surface could be reactivated by techniques such as breath upon the fat left by the fingerprint upon the sensor's surface or applying pressure from a water-filled plastic bag on the sensor's surface (Thalheim, Krissler and Ziegler, 2002). One possible way to prevent this type of security breach would be to design a mechanism to clean the sensor surface after each use.

Certain face recognition systems can be outfoxed by presenting to the webcam (image acquisition device of the system) the digital image of the person with access rights, as long as the resolution matches the requirement of the system and the appropriate distance between the webcam and the display of the digital image is found. More advanced face recognition system can detect live person based on the movement made by the subject. However, it was shown that this could be easily fooled as well by using simple video clips that show the moving head of a person (Thalheim, Krissler and Ziegler, 2002).

The seriousness of biometric security concerns is not an exaggeration taken out of science fictions because biometrics is something unique and cannot be changed. The consequence of biometric data being known or obtained by someone with malicious intentions is permanently disastrous. Imagine someone out there is going to be you forever anytime, anywhere, doing things you never would have done in your whole life!

Ease Of Use

An effective biometric system should have both the features of strong security function and ease of use. These two aspects are mutually dependent and correlate with each other. In fact, one of the advantages of biometrics over password and token is that the user no longer needs to carry with them anything or to remember anything. If the biometric systems somehow were not user-

friendly and hard to use, it would be difficult for biometrics to gain a larger market share. The ease of use of a biometric system can be assessed by asking questions like:

- How long does it take to train a user to use the system?
- How much time is needed for each enrollment/verification/identification process?
- Is it easy or convenient to submit biometric samples without much restrictions/limitations imposed and reiterations needed?
- Are the devices ergonomically designed to protect the health of the users?
- For personal usage, are the devices convenient to be carried around?
- Is the product compliant and interoperable with the various computer platform and devices?
- How easy is it to maintain the system?
- What is the scalability of the system?

Ironically, sometimes user convenience is only achieved by sacrificing certain extent of security. For example, in order to reduce the number of times of asking the users to resubmit biometric samples, a lower threshold value is needed. This would mean that both the users and the impersonators can get through the verification very easily and hence leads to the downgrade of the system's security.

Availability

Another aspect to pay attention to is the availability of the biometric system. A system that is not available for service most of the time would be useless, regardless of the high security functions and ease of use of the system. The unavailability of the system not only jeopardizes the whole information infrastructure, it also increases the cost of troubleshooting, the cost of maintaining a second authentication system, loss in production time, and worst of all could possibly result in fatal accidents at times of emergency such as those systems used in medical centers.

Social Challenges: Public concerns

Privacy

Although biometrics is regarded as the highest level of security, it is still not widely implemented in public except in high security organizations such as the military, public services departments and companies with high security awareness. Despite the considerations of costs and maturity of the technology, public acceptance is one big issue to be addressed before biometrics can fully replace password scheme. The concerns mainly consist of privacy and dignity.

There is fear among public that widespread use of biometrics will invade individual privacy and freedom. It is envisaged that in the future, everyone will be using biometrics to authenticate oneself for most of the business transactions, travel, registration, medical program, report to work and other aspects of life. While it maybe convenient in enhancing security, people are afraid that their daily action and movement are monitored by governments who want to completely control the people in the name of fighting against crimes and terrorism, or by business firms who are interested in knowing the buying pattern and credit history of the customers.

The implementation of various types of biometrics for different applications would imply that people have to leave various physical information such as fingerprints, iris pattern and hand geometry on the network. The existence of central biometric databases heightens the fear because it is possible that all the databases might be linked and data might be exchanged among interested parties to create comprehensive profiles of individuals. The scary part is that all of these can be done without the consent or knowledge of the individuals concerned.

Permanent identity theft is yet another frightening issue, because biometrics is "something cannot be changed". Impersonation through the use of one's biometrics would result in the complete loss of identity and irreversible damage of trust the victim had built in the society.

When biometric data is being misused, freedom of action and thought are likened to that during the time of master and slave because everyone will be more cautious in everyday life. For example, not to read or buy politically sensitive materials, not to leave fingerprints everywhere, walk uneasily (accordingly, there will be technology to identify people based on their walking patterns!!), and feel uncomfortable to see psychiatrists due to constant self-consciousness that they are being monitored.

New York, the spot of September 11 2001 tragedy, has witnessed the installation of more Closed Circuit TVs (CCTV) around the city. This has resulted in quite a stir among the residents. The ordinary publics are worried that the personnel will use the data for other purposes such as spying on neighbors or spouse rather than identifying suspicious criminals or terrorist. A group of technologist from the Institute for Applied Autonomy together with New York Surveillance Camera Project developed iSee, a service that is similar to Mapquest, but provides the users with the routes with the least monitoring camera to their desired destinations (Baard, 2001). One may laugh at the news but it reveals a rather upsetting situation where it is possible that people have to find alternative routes just to get to a place without being monitored.

Dignity

Another reason why the public are not quite ready to accept the biometric technology is the linkage of the application to the history of criminal identification, such as the one using photos and fingerprints to recognize a crime suspect. It is about the question of dignity, about how bad people would feel being treated as suspects and about why they are not trusted. A very well known case that outrages the public's sense of dignity was the covert use of face scanning device during the SuperBowl at Tampa to detect the appearance of criminals and terrorists (Trigaux, 2001). The response from an irritated public should teach all who wishes to introduce biometric application a lesson that it is wiser to get the consent from the users prior to the implementation.

Self-dignity is further challenged when a user is not able to provide the biometric sample in conditions such as lost of finger, blind, dumb or paralyzed. These people will have to be reverted to the second authentication scheme such as password scheme but the feeling of being different, inferior and alienated will discourage them from mixing well with the rest of the society.

Religion and Health

Objections to the use of biometrics also come from certain religious and cultural groups because biometric data is taken as something very intrinsic to human. The idea of identifying a person by closely examining his/her body part is likened to recognizing products or animals by the tag associated to them.

The public also shows anxiety towards certain biometric applications that use technologies unfamiliar to them, for example the use of infrared light to scan the retina pattern of human eyes. The underlying reason for the fear is that the system might be hazardous to their health.

Do You Have A Choice?

The suggestion to let the users have the choice of whether or not to participate in a biometric security system is arguable. If users are given the freedom to choose, then the whole purpose of enhancing the information system security of an organization would be lost since the whole system is as weak as before if the previous authentication system is still in place. Besides, the cost of maintaining multiple authentication systems is also higher. On the other hand, mandatory enrollment in the biometric system would cause disturbance among users who are unwilling to participate, which creates other issues such as loss of customers and depression among employees.

Amidst all these objections and disturbing issues, the biometric vendors and developers are putting much more effort in convincing the public about the benefits of using biometric technologies. Other non-commercial organizations and institutions are also conducting research and publications to facilitate the acceptance of biometrics by all parties.

Policies and Regulations

As with other kinds of technologies, biometrics itself is by no means privacy-invasive. It is the misuse of the biometric data such as disclosure to third party without consent from the users or use of the data for reasons beyond the original intentions, which is horrifying. After all, the human mind is the source of all evils, or why would we ever need a firewall or password to defend against all sorts of attacks from another human being? Privacy policies and better still, regulations should be in place and strictly enforced to ensure that the privacy rights of the people are protected.

The policies or regulations should at minimum cover the following issues (IBG, 2002; Cavoukian, 1999):

1. Collection of biometric data:
   Biometric data should be collected from the users in an open manner and prior to that, users must be notified and consent obtained.

2. Encryption of biometric data:
   All biometric data must be encrypted during the transmission over the network and inside the storage media such as database or tokens.

3. Universal unique identifier:
   Biometric data should never be used as a universal unique identifier, which facilitates linkage to other databases and creation of the complex user profiles.

4. Biometric templates:
   All biometric templates should only exist in formats that are not identifiable without the use of vendors' algorithm, which is to say no raw image of the biometric data should be kept. In addition, the design of the system should ensure that reconstruction of the biometric raw image from the template is impossible. This would ensure that even if the templates were stolen, there would be no means to tell to whom those data belong.

5. Storage of biometric data:
   Only biometric data that are required for the authentication/identification purposes are stored. Any redundant or non-matching data should be deleted. For example, the biometric data of a resigned employee should be eliminated from the database as soon as he/she leaves the company. Furthermore, biometric data should be stored separately from all other personal identifiers such as names or address, which leads to the immediate identification of the person.

6. Authorized access to database:

Access to the biometric database should be limited only to the administrators. Privacy can be enhanced by ensuring that the administrative functions are distributed among a few administrators, thus eliminating the risk of full control by a single person.

7. Disclosure of biometric data:
   Disclosure should be strictly prohibited except in very special cases of which any request to obtain the information by the external parties such as police should obtain a warrant or court order beforehand.

8. Protection of biometric system:
   Security equipments and measures should be used to protect the system from being attacked. This includes the physical security implemented at the facilities that host the database and the protocols used to ensure the safe transmission of data over network.

9. Penalties:
   The regulations should be strictly enforced and penalties should be given to whoever that violates the law.

Be Prepared!

All parties who are involved with biometric applications should work together and produce guidelines for proper actions to be taken in the case of biometric data theft. There is always a possibility of fraud happening even though the system is designed to withstand attacks or such that templates cannot be reverse engineered to raw image.

Questions that need to be addressed include can the victim continue using his/her biometrics or access shall be denied until the impersonator is captured? Is there a second authentication system to be used by the victim and how fast can he/she get used to it? For example if the second authentication system is a password system, can the victim still remember the password since he/she has adopted the biometric authentication for long. What are the proper ways to notify other organizations that use the same biometric product and of which the victim has enrolled in the system, in order to prevent further fraudulences conducted by the impersonator. A good deal of preparation should be made well ahead to avoid panics and more severe conditions due to improper actions in times of security breach.

Trends

As expected, the once powerful one-factor authentication now appears to be insufficient or too weak to face the challenges of computer fraudulences. As a

natural way, two-factors authentications and the latest three-factors authentications are introduced. Biometrics is viewed as invaluable in providing an extra barrier to the existing security measures such as smart card based technology. Hence, there are intensive research works to integrate biometrics into other technologies. One of the latest results is the combination of PKI, smart card and biometrics to provide a strong three factors authentication scheme (Liu and Silverman, 2001).

Another version of biometrics, microchip implantation, turns out to be more offensive to the public than any other biometric technology because this is not the natural form of human biometrics. Extra care and thoughts are needed prior to the introduction of the technology to the public.

DNA profiling, a technology that identifies a person based on the unique characteristics of DNA, have long been used in the forensic industry. Its use in other areas are quite restricted because each verification process requires the user to submit a sample of cells and the analysis process also takes a longer time such that a real time matching is not yet feasible. However, it is possible that the progress of technology will one day bring DNA profiling to the computer world.

A little thought here - if human cloning is possible in the future, how are DNA and generally all other biometric technology going to defend their titles as the unique characteristics of every single human being? If the day ever comes, probably everyone will need to have microchip embedded to differentiate oneself from one's cloned-self.

Conclusion

At its infancy, current biometric technology is still considered immature to completely replace password and other authentication schemes. Security wise, biometric technology shows vulnerabilities that can be easily exploited for wrongful purposes. Biometrics itself is by nature complicated and distinctively secured to each unique identity. It is the imperfect design of the system and its elements that produces the security holes. Hence, to achieve higher security performance, the design of biometric system should take into consideration the possible vulnerabilities of the processes and algorithms of the system for the whole life cycle, namely data collection, data transmission, storage, templates comparison and susceptibility of the system to physical human attack.

Another challenge confronting biometrics is the fact that people are not ready to accept the technology in its entirety. Due to the far-reaching impact of biometric data misuse, any irresponsible use of the technology could be destructive to the society and would certainly compromise the privacy rights of people. Thus,

regulations are needed to control and manage the implementation of biometrics. More issues will arise following the growth in the varieties of biometric technologies. 3-factors authentication, microchip implantation and DNA profiling are among the many that deserve attention.

Although the challenges confronting biometrics are many, none of these is going to stop the progress of biometrics being used as authentication and identification tools. This is not the time to argue whether biometrics should be used widely or not in the future. A wiser approach would be to prepare the people mentally and psychologically for the new technology, make further improvements to the technology itself and think of how to properly use biometrics for everybody's benefit.

References:

1. Baard, Erik. "Routes of Least Surveillance." 28 November 2001 URL: http://www.wired.com/news/privacy/0,1848,48664,00.html (28 June 2002)

2. Cardwell, Andrew. "Biometric Authentication." 28 September 2001. URL: http://www.itsecurity.com/papers/cardwell.htm (29 June 2002)

3. Cavoukian, Ann. "Privacy and Biometrics." September 1999. URL: http://www.pco.org.hk/english/infocentre/files/cakoukian-paper.doc (29 June 2002)

4. Clarke, Roger. "Biometrics and Privacy." 15 April 2001. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (28 June 2002)

5. Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." December 1994. URL:http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html (28 June 2002)

6. International Biometric Group. "FAQ's and Definitions" 2002. URL: http://bioprivacy.org/index.htm (29 June 2002)

7. International Biometric Group. "IBG's BioPrivacy Best Practices." 2002. URL: http://bioprivacy.org/index.htm (29 June 2002)

8. Leyden, John. "Gummi bears defeat fingerprint sensors." 16 May 2002. URL: http://www.theregister.co.uk/content/55/25300.html (29 June 2002)

9. Liu, Simon and Silverman, Mark. “A Practical Guide to Biometric Security Technology.” 2001.
URL: http://computer.org/itpro/homepage/Jan_Feb01/security3.htm
(29 June 2002)

10. Scheeres, Julia. “Airport Face Scanner Failed” 16 May 2002
URL: http://www.wired.com/news/privacy/0,1848,52563,00.html (28 June 2002)

11. Soto, Carlos A. “ Biometric Security Not Quite Ready to Replace Passwords” 2 May 2002.
URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A18474-2002May1&notFound=true (29 June 2002)

12. Thalheim, Lisa; Krissler, Jan and Ziegler, Peter-Michael. “Body Check.” 22 May 2002.
URL: http://www.heise.de/ct/english/02/11/114/ (28 June 2002)

13. Tomko, George. “Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?” 15 September 1998.
URL: http://www.dss.state.ct.us/digital/tomko.htm (28 June 2002)

14. Trigaux, Robert. “Cameras scanned fans for criminals.” 31 January 2001.
URL:http://www.sptimes.com/News/013101/TampaBay/Cameras_scanned_fans_.shtml (29 June 2002)