GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Michael Zimmerman
Version 1.2f

BIOMETRICS AND USER AUTHENTICATION

From the casual user of the home computer, to businesses, corporations, medical professionals/providers, and government, there is a great concern about the security of files, systems, and the ability of technology to protect us from unauthorized access. Computer software companies and those in research and development are scrambling to meet the demand for better security of sensitive, confidential, and classified information.

A great deal of research has already been completed and the results are available for review both on the Internet, in various periodicals, and books. Information is also available from tech companies who are designing specific software or other security applications for the protection of sensitive and confidential materials. The catastrophic events of September 11, 2001, have certainly had an impact on how we view security in the day of technology, and whether or not technology can give us the protection we need from unauthorized invasions of our privacy. It seems to make sense that biometrics technology will be at the forefront of existing and new security measures in the world of Information Technology.

Introduction:

One of our highest priorities in the world of information security is confirmation that a person accessing sensitive, confidential, or classified information is authorized to do so. Such access is usually accomplished by a person's proving their identity by the use of some means or method of authentication. Simply put, a person must be able to validate who they say they are before accessing information, and if the person is unable to do so, access will be denied. Generally speaking, a system can identify you as an authorized user in one of three ways – what you know, what you have, or what you are. The most widely used of the three methods is what we know – passwords or other personal information. A more sophisticated method of authentication is what we have – smart cards and tokens. The last method is what we are - biometrics technology. **(1)**

Biometrics systems can identify users based on either physiological or behavioral characteristics. Again, the events of September 11, 2001, have spurred a great deal of interest in further enhancement or refinement of this technology. Individuals are concerned that security systems be put in place that would prevent unauthorized access to personal data, and that their identities cannot be stolen and used by other individuals. At present, biometrics technology holds a great deal of promise for doing just that, but is not without its limitations and certainly not without its critics.

Biometrics is a field of technology which has been and is being used in the identification of individuals based on some physical attribute. As funding for research has permitted there has been an effort by several tech companies to develop standards for hardware and software that would be used throughout the industry in further development within this area. The purpose of

© SANS Institute 2000 - 2005 Author retains full rights.

this paper will be to look at the use of biometrics technology to determine how secure it might be in authenticating users, and how the users job function or role would impact the authentication process or protocol. We will also examine personal issues of privacy in the methods used for authentication; the cost of implementing a biometrics authentication system; the efficiency of biometrics authentication; and the potential for false positive or negative recognition of individual users.

Biometrics Authentication

Generally speaking, there are four factors of physical attributes that are used or can be used in user authentication:

- Finger print scans, which have been in use for many years by law enforcement and other government agencies and is regarded as a reliable, unique identifier.

- Retina or iris scans, which have been used to confirm a persons identity by analyzing the arrangement of blood vessels in the retina or patterns of color in the iris

- Voice recognition, which uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.

- Facial recognition, which use unique facial features to identify an individual. (2) **Antari, INC**

Biometrics and Privacy Issues

There are two ways to examine this concern among users. One has to do with the actual steps necessary to authenticate the individual user, and the other with the overall concern for privacy and how unique identifiers will be used.

Face recognition and retinal scans are areas that have the potential for making users feel very uncomfortable when used for the purpose of authentication. We tend to think of this technology in terms of the ability of a system to match a photograph or the eye to a particular individual, and indeed that is the premise. However, in order to do this, the system may require an individual to come in very close contact with a camera or a scanner during the authentication process. Some people find this method of authentication too intrusive of their personal space. Although this method of authentication feels very intrusive to some, it is not a major concern for the majority of users.

The majority of expressed concerns relate to privacy issues of the individual user. Specifically, users are concerned with how and where information is stored; who can access it; how it can be used; and the reliability of its usage. These concerns are certainly valid for persons who view biometrics technology in its most broad sense, but are not as valid when applied to user authentication. The difference is in how this technology is used. For the purpose of authenticating an individual user, the system does not try to determine the user's identity – only

© SANS Institute 2000 - 2005 Author retains full rights.

to confirm it. It will only allow access by a user to a particular application or network when a match is confirmed. The method of storage is also different from an actual finger print or photograph that might be on file. For user authentication purposes, data is stored as a mathematical representation **that** cannot, in and of itself, recreate the original image. **(2)**

Storage of unique identifiers is also a concern to some individuals. Information can be stored locally which provides for easier access and control, and lessens the concern about network attack. **(1) Another** method of storage is centralization of data, which can make the information more vulnerable to outside attack. Smart card storage of data is another method of storage, and puts the information within the control of the user. While this may feel more comfortable to the individual, it poses a number of security risks and should not be used by itself for authentication purposes when accessing sensitive, confidential, or classified information. Interestingly enough, laws in some countries require that the information be stored on tokens or smart cards.

Biometrics Efficiency

Biometrics technology is without a doubt a more efficient way of authentication than the more common use of pass words, smart cards, or a combination of the two. Potentially, the user would not have to remember a password or a series of passwords to access information. Passwords also have expiration dates that require new assignment of passwords and more work for technical support staff. Businesses, corporations, and medical providers have found that too many times users cannot remember their pass words, and trying to navigate through a series of steps to access needed information becomes cumbersome and time consuming. Technical support staff can be kept busy providing instruction to individual users who have difficulty with the technology associated with even some of the more basic procedures of signing on or logging on to a particular application or network.

Biometrics is a promising technology that is being touted as the solution to these problems. **In systems that use single sign-on, this particular technology would be a very efficient way to authenticate the user.** You save time and resources when you have "the ability to authenticate just once and be properly recognized." **(3)** This approach "consolidates multiple user identities into a single identity that can be used everywhere. That means each user has access to multiple networks and applications after logging in once." **(2)** More and more businesses and corporations are recognizing the efficiency of such an application. In hospital settings for instance, there is more and more interest in using biometrics for user authentication to assure the confidentiality, privacy, of patient information.

There is also a down side to the question of efficiency in the use of biometrics in the authentication process. Research has shown that no system is perfect and biometrics in its present stage of development is no exception. Although false positive and negative identification will be discussed as a separate security issue, it also has implications to the user who needs to **sign-in** or log on and is locked out because the system does not recognize the user as being legitimate. When this occurs, time can be lost both by the individual user and the technical support staff in identifying and rectifying the problem(s).

© SANS Institute 2000 - 2005 Author retains full rights.

When different products were tested to determine how securely and efficiently they could authenticate users, varying results were obtained. For instance, face recognition systems could be fooled by the use of a mask. With some systems tested, it was necessary to increase the confidence levels to prevent unauthorized access. The downside according to the researchers was that "an increase in the certainty threshold translated into a longer authentication process and an increase in the frequency of false rejections." **(4)** This would decrease some of the benefits related to efficiency, but would not be a compelling reason to discount its overall benefits. What the biometric industry is working toward is a "complete replacement for your password and cards." **(5)** **While** this statement was not directly related to user authentication, it certainly applies. Companies involved in research and development would indeed like to develop a system that completely replaces passwords and cards while insuring the integrity of sensitive data and information.

Biometric Security Issues

Although there has been substantial research related to security issues there is still more to be done. We have mentioned some of the security issues previously as they relate to privacy for the individual user as well as the efficiency of biometrics in user authentication. A more in-depth examination would indicate that there are areas that warrant concern. For instance, we need to understand how vulnerable data are to theft or abuse; how the data are to be retained to optimize the security of the data; whether the information can be tampered with; and how much of an error factor in the authentication process is acceptable.

In an article published in PC Magazine (on line) in February 1999, biometrics security was examined. Benchmark testing results of finger print recognition, face recognition, and voice recognition were reviewed. Efforts were made to determine how secure the factors were in authenticating users by subjecting products to various test scenarios. Finger print recognition proved to be the most secure of the products subjected to the testing and there was no success in any of the efforts made to fool the device.

Face recognition systems could be fooled with a mask at the default settings, but as the threshold levels were increased to above 96 percent confidence, no system tested allowed entry. As previously stated, legitimate users were locked out when the higher threshold level was used.

Only two voice recognition products were tested and one allowed an unauthorized user to get in. However, the testing result of that particular product is somewhat questionable. They did not use the microphone voicecrypt recommended for the test because it was not in stock. **(4)**

A biometrics integration and consulting firm known as International Biometrics Group has worked with the private sector, with government, and with medical professionals in evaluating various biometrics technologies. They have conducted comparison testing in fingerprint, facial recognition, iris recognition, and voice recognition. One of the systems evaluated was the face

© SANS Institute 2000 - 2005 Author retains full rights.

recognition system developed by a corporation in Burlington, Ontario. When tested, their system had a 0 percent False Acceptance Rate and a 3.1 percent False Negative Rate. This rate of failure of a system to authenticate authorized users may be an acceptable rate for some but not for others. Clearly it would depend on your job function as to how problematic this might be, and how much time would be lost when this occurs. This same corporation has an exclusive license for the use of a very sophisticated technology known as Holographic Quantum Neural Technology that is to be used in future face recognition technology. **(6)**

The International Biometrics Group has also evaluated the effectiveness of Iris and Retinal scan technology. This technology is not new and has been in use for approximately (15) fifteen years. Testing of products indicate that retinal scans are not easily fooled. Although it would be difficult to replicate the retina, it is possible to gain unauthorized access by such an act. In one discussion about retinal scans, it was mentioned that removal of the eye would be another way to breach security. Both of these risks would be effectively eliminated by using a thermal scanner that measures heat. This type of scanner is often used with the fingerprints.

Iris scans are also a very effective way of authenticating a user, but there are issues which affect this particular technology. For instance, the eye must have a certain degree of lighting to allow the camera to capture the iris. **(6)**There is potential for failure when enough light is not available. We have to remember that in real world applications of any technology, environments in which work is performed can be very different and in some cases make a particular method of user authentication contraindicated. Lighting issues not withstanding, the iris scan technology is viewed as a very reliable method of authentication when subjected to testing.

Biometrics technology does not in and of itself protect against internal or external attacks in user authentication systems. In order to guard against such attacks, steps should be taken to protect authentication information. Systems that store biometrics data and credentials should do so in encrypted format by using a Public Key Infrastructure **(2)** Audit logs should also be kept with a high degree of detail required. Such logs should be able to detect if a user does something that is questionable, and that would compromise security. Standards should also be in place that would prevent one person from compromising the systems ability to identify a user who has committed an inappropriate act **(2)** Finally, security is enhanced when the software that performs the authentication function is not located at the users work station. The data should be entered at the workstation, but then passed on to a secure server for authentication. This decreases the possibility that the data can be tampered with. **(2)**

Biometrics and Job Function/Roles

When using biometrics technology, or any other technology for the purpose of verifying a user's identity, it is important to understand that not everyone within an organization or department needs access to all information. While biometrics is considered the most reliable form of user authentication, we must remember that user authentication is complex, especially when applied to a network where one person may need to have access to various applications or systems.

© SANS Institute 2000 - 2005 Author retains full rights.

People within organizations who need access to sensitive, confidential, or classified information will need the strongest form of authentication - three-factor authentication. This level of authentication will necessitate use of passwords, smart cards or tokens, and personal identifiers. Those who need to have rapid access to a particular application or system might need to use a smart card or token. A password may be the only authentication needed for those with minimal security needs.

A person's specific job duties or work environment will also impact user authentication. For example, in a manufacturing environment where noise levels are high or heavy glovers are being worn voice scans or finger print scans would not be appropriate. The point is this - there is a need for flexibility in any authentication protocol that can accommodate different workplace constraints.

Biometrics and Cost

As biometrics technology moves from research and development to implementation in the market place, cost to users of the technology has to be a concern. All of the issues related to Y2K meant that many organizations, corporation, and government entities had to expend a major portion of their Information Management budgets to upgrade their systems prior to the year 2000. Systems that were upgraded 3 and 4 years ago may need to be reevaluated to further eliminate any security risks to the systems.

A security evaluation may reveal user authentication as one of the vulnerable areas needing to be upgraded. Biometrics technology may be considered as a solution to stronger user authentication in such a scenario. Most products are designed to integrate with existing systems without having to replace all of the existing hardware and/or software. Certainly any upgrades would not require the kind of capital expenditures associated with Y2K.

One of the advantages to using biometrics technology for user authentication is its low cost with finger print technology costing as low as $100.00. However, the cost of using a retina scan device can be $2,000.00 - $2,500.00 and puts it at the other extreme of the cost spectrum. This has proven to be one of the factors that make this type of technology less attractive to most potential users, even though it is highly reliable.

One has to also factor in the cost of not making a change to biometrics technology in calculating help desk time for users who simply have forgotten their passwords, and this happens a lot. According to one source, such calls can cost “upwards to $35 a shot.” **(8)** Other cost factors for technical support staff include reassigning passwords that have expired when the system does not assign the password for the user. There is also a cost factor if passwords are stolen and there is a breech in security. Stolen passwords can result in lose of money and while biometrics technology may not completely solve all of the cost related problems, it will certainly decrease it.

Conclusion

© SANS Institute 2000 - 2005 Author retains full rights.

While biometrics technology provides a strong user authentication solution, there are other variables to be considered in the authentication protocol. When a high level of security is needed, it is recommended that you combine other authentication factors with biometrics. When you combine what you know, what you have, and what you are, you will have achieved the highest level of security across multiple applications and systems. According to information made available by the International Biometrics Group, "there is no one right biometrics technology for every application." **(9)**

References:

1. Biometrics, Aidan Dysart
   http://www.zdnet.com/pcmag/features/biometrics/bench.html

2. The Challenge of User Authentication
   http://www.ankari.com/whitepapers.asp

3. NMAS Implementation Scenarios
   http://developer.novell.com/research/appnotes/2001/july/01/a0107015.htm

4. Benchmark Test
   http://www.zdnet.com/pcmag/features/biometrics/bench.html

5. Body may be key to foolproof ID
   http://www.usatoday.com/life/cyber/tech/ctc447.htm

6. AcSys Biometrics Produces Excellent Results On IBG Test
   0% False Acceptance Rate and 3.1% False Rejection Rate
   http://www.nxsgrp.com/html/press_releases/nxs_release_09_04_01.html

7. Iris Recognition: Issues
   http://www.iris-scan.com/iris_cautionary.htm

8. Hardware prices dropping but user acceptance low.(biometrics)(Industry Trend or Event)
   http://www.findarticles.com/cf_dls/m0CGC/15_25/54413163/p1/article.jhtml

9. The Zephyr™ Charts
   http://www.biometricgroup.com/e/zephyr_charts.htm

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: April 27th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS