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

Mark W. Wolansky
GSEC Practical Assignment
Version 1.2b

Stronger Authentication Methods: Biometrics and Public Acceptance

Accounts of major computer systems being compromised in some form or another make big news stories. When Microsoft gets hacked, the whole world notices. Unfortunately, for every time this type of story gains national media attention, there are hundreds, perhaps even thousands of instances of intrusion which are discovered that don't make it to the 5 O'clock news. Even more distressing is the untold numbers of intrusions that are not detected or detected and not reported. Attacks like these threaten the privacy of everyone, people and institutions alike. They bring with them the growing threat of identity theft. High tech criminals are stealing people's electronic identities to log into computer systems, use their credit cards, access bank accounts, or a host of other fraudulent activities. This is not only a threat to the public but to corporations as well. No bank wants to be known for not protecting the account information of its patrons. Likewise no company want's to be in the news as the victim of the latest big hack or virus. Based on this it is apparent that the need for better electronic security becomes more urgent every day. A stronger method of authentication to prove the legitimacy of a transaction other then the typical use of passwords is one way to strengthen security. One technology advancement that has the potential to bring stronger authentication and improved security is biometrics. Just enabling stronger authentication is not necessarily the biggest obstacle faced in improving electronic security, the hard part is gaining public acceptance.

Biometrics is quite simply the use of some measurable, unique, physical attribute for authentication. The most common example of biometrics would be a fingerprint. Other examples are the patterns of blood vessels in the retina of the eye, the subtle differences in the iris of the eye, a palm print, facial recognition, hand geometry or voice print analysis. Many of these technologies are still in development, so they are seen in science fiction more than in the real world. However, biometrics, used as an authentication measure, has the potential to greatly increase the degree of security in many of the systems we use in everyday life. Before we can understand how biometrics can help improve security, we must understand authentication and how biometrics could fit into the authentication procedure.

Authentication is the key to security of any kind. In order to gain access to a safe a combination is needed; to enter a locked door a key is required; to enter a secure building credentials and the trust and recognition of the guard is necessary. Authentication in the realm of information security is the process by

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

which a system can determine whether or not a given person or computer system is who they claim to be. Electronic authentication for information security is invaluable, if your authentication is compromised the rest of your security measures are bypassed as well. For that reason it is of the utmost importance that we ensure that authentication is as secure as possible and find ways to implement publicly acceptable secure authentication methods.

One of the best ways to increase the security level of authentication is to move from one-factor authentication like a password to two-factor authentication like a password and something else. It is the something else that is important. The authentication criteria can be drawn from three sources:

- Something you know. – This could be a password, a PIN, mother's maiden name, city of birth or anything else that would be unlikely for a stranger to know.
- Something you have. - This would be some type of device used for authentication, this can also be referred to as a security token.
- Something you are. - This would be your hand, your face, your voice, your eyes or any other measurable physical attribute that is unique to you.

There are two types of two-factor authentication. One is a combination of 'something you know' and 'something you have'. The other is a combination of 'something you know' and 'something you are'. Two-factor authentication using 'something you have' is achieved using a security token of some kind. The security token is typically an electronic device, like a smart card, with information that needs to be accessed in some way during authentication. Two-factor authentication using 'something you are' is biometrics. Biometric authentication systems use information based on some kind of physical measurement of your body. This data is then stored in a template to be used for comparison against data that is collecting during an authentication attempt.

Why do we need to use two-factor authentication? One-factor or password authentication may not be strong enough for many situations. The problem with simple password authentication is human nature. In general we do not like to remember more than we have to. When it comes to selecting a password we have a tendency to pick something that is easy to remember and/or easy to type. Unfortunately if the password is easy to remember or type it is usually also easy to guess (or crack) and opens up a potential security breach. One possible solution to this would be to require users to use more complex, strong passwords. Unfortunately that creates another problem: people don't remember the more complex, strong passwords. Many people write down even their simple passwords, consequently, more complex passwords are even more likely to get written down, left on desks, under keyboards, or even stuck to the monitor! Again this opens up a potentially serious risk. Even if you can get everyone to use strong passwords and remember them without writing them down, you still

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

have a potential for breach via social engineering. Social engineering could be as simple as someone asking for and receiving a password or a more complex scheme involving someone pretending to be a bank representative and asking for account information over the phone.

Two-factor authentication using biometrics may very well be the key to increasing the security of the information we use everyday. Biometric based two-factor authentication has several advantages over two-factor authentication using a security token. Security tokens can be lost, stolen, or sometimes even duplicated. Also, security tokens are something else that needs to be remembered. It is quite annoying to go to the ATM and realized you left your ATM card on the dresser. Likewise it would be frustrating to need your security token and not have it with you. When using biometrics as the second factor in two-factor authentication the factor is 'something you are', therefore, you can not forget to bring it with you. (I hate when I leave my hands on the dresser in the morning!) It is also very hard for someone to duplicate or steal the means for biometric authentication. If presented in the right way, perhaps the public could accept the added security with the convenience of not adding another object to carry with them every day.

Unfortunately, we are still on the cusp of the age of biometrics. It is apparent that using biometrics in conjunction with a password is much more secure than a password alone. It would also seem that biometrics is a better method for implementing two-factor authentication than using security tokens. So the question becomes: How do we move biometrics from the realm of science fiction to science fact? Science fiction may be part of the problem, biometrics is often tainted by its portrayal in science fiction movies. It is often portrayed as part of a complex and sometimes invasive security system. In general people don't want to be bothered with anything they perceive to be too complex. They don't feel the level of security used by covert militaristic organizations is necessary in the lives of everyday people who don't have secret documents and stolen gems to protect. Thus biometrics is perceived as being complex and excessive and faces a challenge in gaining public acceptance. Another area where movies hinder acceptance of biometrics is convincing people that biometrics is, in fact, more secure. In many movies, biometrics are frequently easily defeated by the likes of James Bond or Ethan Hunt. It seems easy enough to the audience to duplicate a finger print on a thin plastic-like material that generally resembles Elmer's glue. What's the point in using biometrics when it seems so easily compromised?

Other areas of public concern that may be fueled by movies, books, media and commonly held 'conspiracy' theories include public safety and privacy. The apparent invasiveness seen in the use of biometrics in some movies may raise public concerns as well. People are against the idea of having 'lasers' (or other light) shined in their eyes to do a retinal scan. Another invasive biometric seen in movies is the DNA scan using a drop of blood drawn from the finger like seen in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the movie Gattaca. Public safety is another threat fueled by these portrayals. The plot to circumvent a biometric scan often involves the murder of a security guard so that the evil spy can use his handprint or something of that sort. People don't realize that a biometric scanner wouldn't recognize a dead hand. The last and most important concern is privacy and the misconceptions that surround it. People are afraid of an 'Orwellian' society in which there is no privacy from the government. It would seem the public is greatly concerned about privacy. However, often the same people who are afraid that big brother is watching are the people who leave their password stuck to the monitor. Nonetheless privacy is a valid concern with biometrics and is something that must be addressed.

Privacy and its perception is a key hurdle that must be overcome in order for biometrics to gain pubic acceptance. There are privacy advocate groups that are making efforts to keep the use of biometrics from becoming common place. One such group is "Fight the Fingerprint" the first line on their web site reads, "We Stand Firmly Opposed to All Government Sanctioned Biometrics and Social Security Number Identification Schemes!" Groups like this use privacy as an angle to help to fuel the fire and try to keep biometrics from becoming a prevalent technology. Many people have concerns that biometrics will be used as a surveillance technology. It can also be seen as another way to dehumanize society and make all of us a series of ones and zeros in a database somewhere. What people fail to realize is that biometrics itself would not be the cause of such a problem. The collection and use of the data for personal security should not be a concern. The concern should lie in the potential misuse of the information collected. When someone begins using biometric authentication for any purpose, it is done with the assumption that the data will only be used to authenticate him or her for access to a specific area or service. The danger in misuse lies in the ability to use a biometric identifier as the means to link several different databases to the same user. This would allow the data to be used for purposes not intended for at the time of collection, this could be refereed to as "function creep". This takes away control that a person has over his or her own information and identity. It is interesting to note that Biometrics can actually be used as means of addressing the issue of "function creep".

There are also technological concerns regarding biometrics that must be addressed before there is a wide spread implementation. Many of these concerns are already being addressed, and have been addressed in other countries. However, it is important to note that these situations exist. One major concern would be the theft of a biometric. Although it is very unlikely, it is possible that someone could compromise a biometric authentication system by somehow impersonating the actual user. This creates an interesting problem because there are no 'password resets' in biometrics once someone has the means to impersonate biometric data that biometric authentication is permanently compromised. This makes it extremely important for biometric data to be secured. It may be possible to minimize the risk of this by ensuring that the means to recreate a biometric is never stored in a database, because if the data

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

exists it can be hacked. Another technology hurdle that needs to be addressed is how to handle dismemberment or death. You only have one left thumbprint and should you for some reason loose your left thumb or anything that it is attached to you no longer have your biometric. Intrinsic to the security of biometrics there should be no way for an administrator to 'reset' a biometric without the active involvement of the authenticated user. There are several ways that this may be addressed. They would most likely need to involve some sort of two sided authentication involving either the user or their heir (or boss in the event of a termination with in a company) and a system administrator to complete a reset of the biometric.

There can never be public acceptance of biometrics until the public feels that their information is safe and won't be misused. One of the keys to this is policy, like a good security policy in a private company; there must be good legislation that protects people's rights. As in a good security policy, the public should be aware of the policy / legislation and thereby aware of the rights they have as a result of the policy / legislation. As always the policy or legislation will mean little if it is not enforced and contain a mechanism to change as the technology or public needs and demands change. Along with the proper laws and policies there must be proper use of the technology. The proper use of this technology must also be enforced with good laws and policies. There are legitimate concerns for the misuse of biometric data. Most of these concerns can be addressed through proper use of the technology. Alan Greenspan is quoted as saying, "Indeed, the most effective means to counter technology's erosion of privacy is technology itself." We need to be sure that a biometric is not used as a global identifier that could potentially link multiple otherwise unrelated databases to the same person. To accomplish this, the actual biometric data should never be stored in any database. Instead biometrics should be used in conjunction with encryption, potentially in a situation where the mathematical representation of the biometric is used as the encryption key. This would insure that the biometric itself could not be used in anyway against the user.

Another key to public acceptance is education. Education is important regardless of whether biometrics is being implemented internally in a company or if it being introduced to the public for use at ATM machines. The people who will be using this technology on a daily basis must be informed so that they understand the benefits as well as the risks of biometrics. Perception is very important here. The users must be shown that the process is safe, secure, and easy to use. If an effort is made to get the public to understand biometrics and not fear it, we will be that much closer to more secure information environments.

In addition to the more superficial concerns there are some psychological issues that must be addressed. Some people subconsciously consider the need to identify oneself distasteful and biometrics takes this to the ultimate level. For many it creates an atmosphere that questions a person's reputation and trustworthiness. Everyone feels more comfortable "where everybody knows your

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

name;" where everyone recognizes your fingerprint is more reminiscent of Big Brother then a friendly neighborhood bar. Also, because of the association of fingerprints with law enforcement providing fingerprint information is sometimes seen as an embarrassment or as an accusation. Therefore it is important that we address the psychological perception of biometrics as well. It must be portrayed as something that is normal and something that every upstanding citizen should want to do to protect his or her identity. Also every step should be taken to ensure that the public is confident that their personal information is safe and that biometrics is part of the means for maintaining that security.

Perception often translates to reality in a person's mind. Public perception of biometric authentication methods can be difficult to overcome. Fears include technological fears that the device may harm them in some way. There are also some religions that may not allow the use of certain biometric devices. Along with the other concerns that have been addressed in this paper it seems that public acceptance may be a daunting task. It is important to recognize that these feelings and fears are not necessarily the norm. Normal or not it does not make these issues go away. With proper laws, policy, education and the proper use of this technology we can gain public acceptance of biometrics. This will make it possible to make a bit of science fiction become reality and our data and identities will be more secure. Now we just need to work on that "Beam me up!" technology.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sources:

Fight the Fingerprint. "Fight the Fingerprint Web Site." URL: http://www.networkusa.org/fingerprint.shtml (5 April 2001)

Fried, Stephen. Information Security: The Big Picture. SANS GIAC 2000. 156 -157

Greenspan, Alan. "Remarks by Chairman Alan Greenspan, Federal Reserve Board, Conference on Privacy in the Information Age." March 7, 1997. URL: http://www.federalreserve.gov/boarddocs/speeches/1997/19970307.htm (10 April 2001)

Gupta, Manoj. "Biometric Technologies Overview." SANS Information Security Reading Room. March 16, 2001. URL: http://www/sans.org/infosecFAQ/authentic/biometric2.htm (5 April 2001)

Gustafson, Dani. "Biometrics: Has its Time Come?" SANS Information Security Reading Room. October 31, 2000. URL: http://www/sans.org/infosecFAQ/authentic/biometrics_time.htm (5 April 2001)

Information and Privacy Commissioner / Ontario. "Consumer Biometric Applications: A Discussion Paper". September 1999. URL: http://www.ipc.on.ca/english/pubpres/sum_pap/papers/cons-bio.htm (4 April 2000)

International Biometric Industry Association (IBIA). "Biometric Technologies Steadily Gain Prominence" March 2, 2001. URL: http://www.ibia.org/pressrelease20.htm (30 March 2001)

Kabay, M.E. Ph.D. "Identification, Authentication and Authorization on the World Wide Web" An ICSA White Paper. October 19, 1998. URL: http://secinf.net/info/www/iaa/iaawww.shtml (10 April 2001)

Liu, Simon and Mark Silverman. "A Practical Guide to Biometric Security Technology" URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (5 April 2001)

Schmidt, Andreas. "Two-Factor Token Authentication on e3000" August 2000. URL: http://www.hillschmidt.de/gbr/twotoken-0008.html (30 March 2001)

U.S. House of Representatives, Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services. "Biometrics and the Future of Money". May 20, 1998. URL: http://commdocs.house.gov/committees/bank/hba48784.000/hba48784_0f.htm (10 April 2001)

Woodward, John D. "Biometric Scanning, Law & Policy: Identifying the Concerns – Drafting the Biometric Blueprint." Copyright 1997 University of Pittsburgh Law Review. URL: http://www.pitt.edu/~lawrev/59-1/woodward.htm (4 April 2001)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: March 30th, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

Mentor Session - SEC401	Hollywood, CA	Apr 07, 2017 - May 05, 2017	Mentor
Mentor Session AW - SEC401	Grand Rapids, MI	Apr 07, 2017 - May 19, 2017	Mentor
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201704,	Apr 11, 2017 - May 18, 2017	vLive
Community SANS Cleveland SEC401	Cleveland, OH	Apr 17, 2017 - Apr 22, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
Community SANS Virginia Beach SEC401*	Virginia Beach, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
Mentor Session - SEC401	Edmonton, AB	Apr 26, 2017 - Jun 07, 2017	Mentor
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
Community SANS Las Vegas SEC401	Las Vegas, NV	May 08, 2017 - May 13, 2017	Community SANS
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
Community SANS Columbia SEC401	Columbia, MD	May 15, 2017 - May 20, 2017	Community SANS
Community SANS Baton Rouge SEC401	Baton Rouge, LA	May 15, 2017 - May 20, 2017	Community SANS
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
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
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event