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 (Security 401)"
at http://www.giac.org/registration/gsec

Authentication - The Migration to Biometrics

Ryan D. Reichenbach
GSEC v1.3

Summary Information
As technology continues to develop, traditional controls used to secure information are quickly becoming obsolete. Strong passwords have long been considered one of the cornerstones of information security. Corporations have spent considerable time, resources, and money on encouraging and enforcing strong passwords.

This paper will explore what is quickly becoming a weak control, the password, and its successor, biometrics. The biometric industry is growing at a healthy pace, but there are hurdles to full-scale implementation. As the industry matures and the general public's fears are eased, we should begin to see biometrics being incorporated into our everyday lives. No single authentication technology will completely secure our computers, but with the right combination we can significantly reduce our risk.

History of Authentication Techniques
As security professionals, our main purpose is to protect our company's systems and information from unauthorized access. To accomplish this goal, it is essential to authenticate every user who attempts to access our information systems. There are three major methods of authenticating a user:

- something the user knows,
- something the user has,
- something about the user.

Traditionally security professionals have relied on the basic password, which is something the user knows.

Something the User Knows – Passwords (1)
Passwords traditionally have been the first line of defense against unauthorized access to systems and sensitive data. Password standards and security settings have long been a difficult compromise between system administrators and the users themselves. As the need for security has increased, standards for passwords have become more restrictive. Today, a "strong" password is often required where users must mix numbers and special characters to slow a potential hacker.

Password secrecy is a fundamental principal of a good security policy. However, setting system configurations to properly enforce strong passwords makes it more difficult for users to remember passwords leading to the user posting them in plain-sight on notepads. Most companies will have password standards defined within their security policies. Common password parameters will look something like the following:

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

- Password Length: 6-8 alphanumeric characters.
- Password Expiration: 30-60 days
- Password Lockout: After three (3) failed attempts
- Password Reuse: System should remember past twelve (12) passwords
- Minimum Password Age: Five (5) days
- Users should be logged out after 20 minutes of inactivity.

The easiest attack on a password is password guessing (brute force). This attack is executed just as it sounds. An attacker keeps trying to guess a password until the correct password is guessed. Users traditionally choose passwords that are easy to remember or point to something in their everyday life; this makes the password easy to remember. Even by setting passwords to the above-mentioned parameters, relying solely on passwords as the backbone to your information security policy is quickly becoming a risky proposition. Even the strongest passwords can be broken if given enough time. Similarly, locking accounts after three-failed login attempts will keep an attacker from making unlimited guesses until they are successful, that alone does not keep the attackers out. Nor does creating what are typically considered "strong" passwords by using a combination of letters, numbers, and special characters (i.e. *,#,%).

Poor system administration practices are the easiest avenue for the attacker to gain control over any system. By leaving default accounts with default passwords on our system, attackers can gain access to systems and the password files, which are stored within. Some systems encrypt the file in which the passwords are stored, however once the attacker has access to the file it could be easily downloaded to the attackers computer, at which time the attacker has all the attempts he needs to guess these passwords. Passwords can also be obtained by other attacks such as login spoofing, replay attacks, and by monitoring the traffic between computers.

Something the User Has – Tokens/Smart Cards [2]

So now that I have painted a picture that may at first look like there is no hope, let's look at what makes up the other two methods we use for identification. First up, the method of using something the person has to identify them as an authorized user. While the main focus of this paper is biometric identification, I want to first take a look at tokens and smart cards as other alternatives to the password. The can be thought of as the link between the traditional password and biometric identification. As we will see tokens aren't perfect, but they are a step above passwords. We will also later look at ways of using multiple authentication methods in combination to better secure information. Tokens will play a role in some of these combinations.

Memory tokens are probably the most common use of this authentication method. One of the common implementations of the token technology is the

© SANS Institute 2000 - 2005 Author retains full rights.

basic magnetic striped card (i.e. credit or ATM cards). This card contains information about the owner of the card. The card itself is used to identify the holder of the card. Tokens are also used in conjunction with the common password or PIN (personal identification number).

One of the more interesting implementations of the memory token technology is the use of this technology on driver's licenses. In part this helps reduce if not eliminate the effectiveness of a fake ID. By placing the token technology on the driver's license, your favorite local sports bar can now use a device similar to the device used to swipe and ATM or credit card to confirm the drivers license is in fact authentic. Some dance clubs, which allow admission to young adults over the age of 18, have begun to use this technology to help protect themselves from serving under age customers. Now of course this won't stop those lucky few who happen to look close enough the their older siblings to "borrow" their Ids for a night out on the town. Some colleges and university have been using the smart card technology for access to buildings and cafeterias for a number of years.

As mentioned earlier, memory tokens play a role in combining authentication methods. They also are bridging the gap to biometrics. As we adjust to the post September 11th world, look for a push towards more uses of this technology by the government. Georgia, North Carolina, and Kentucky, to name a few, have already integrated biometrics into their driver's licenses.(9)

Smart tokens provide an additional element of security with the use of one-time passwords. When most people think of token technology in the security world, it is the smart tokens, which comes to mind first. There are three main smart token protocols that determine the level of security provided by the device. The first protocol is the basic static password exchange. With this protocol the user authenticates to the smart token which in turn authenticates to the computer. The static tokens work much like the memory tokens noted above. The key to these devices is the PIN, which is entered by the user.

Another protocol used in the smart token technologies is the dynamic password generator scheme. This protocol uses a password (usually composed of numeric characters) generated by the token at regular intervals (i.e. every minute). The user can then enter the password into the computer, or if the token has an electronic interface, the password is sent automatically to the computer for authentication.

The third protocol is the challenge-response. With this protocol the computer generates a random set of numbers which the smart token uses to generate a response to the computer that is used for authentication.

The main advantages to the smart token technology are that in the case of the challenge-response and password generator schemes we have the one-time

© SANS Institute 2000 - 2005 Author retains full rights.

passwords. The technology also allows us to take advantage of two of the methods of authentication, something the user knows and something the user has. But, as with any technology, there are some disadvantages. The main disadvantage being the cost of token replacement along with the cost of the readers for the electronic interface tokens. There is also a fair amount of administration involved in the use of the smart token technologies.

Something About the User – Biometrics (2)

We have covered two of the three authentication methodologies and have seen that each still leaves systems vulnerable. Passwords can be guessed, cracked, or stolen. Smart tokens and memory cards can be stolen and usually require a significant amount of administration. So, what's left? The third authentication method is something about the user. This is where biometrics enter the picture.

There are six major means of biometric authentication:

- Fingerprints
- Hand Geometry
- Signature Dynamics
- Voice Verification
- Iris/Retina Scanning
- Face

Each has advantages and disadvantages. The success of any biometric authentication device lies in its accuracy. Authentication errors can be classified as either Type I or Type II error. Type I errors are the rejection of authorized individuals. This can happen due to a number of reasons such as degradation of the scanning equipment and changes in the sources of identifiable information (i.e., change in voice or in finger lengths). Type II errors are defined as acceptance of imposters as authorized users. While the likelihood of an imposter gaining access to a system using biometric authentication is lower than the likelihood of access to a system using the traditional password authentication, the possibility still exists (more on this later).

Fingerprints (2)

The main identifiers in a fingerprint scan are called minutiae, the detailed features that can be identified by a trained examiner. Traditionally when we think of fingerprinting technology we think of the law enforcement community and forensic work. Everyone has seen a TV show or movie where the detectives are dusting a room for fingerprints to identify the criminal. With the advancement of the computer industry the fingerprint can now be entered into a computer where it is scanned against a database of known fingerprints to find a match. In the authentication arena, the fingerprint is captured without the use of inks. The user presses his/her finger against a scanning pad. The fingerprint is recorded and immediately compared to the images stored on a database. If a match is found, the person is authenticated and allowed to continue. If no match is found, access is then denied. The fingerprint scan is often used in conjunction with the traditional access card. The user first presents the access

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

card to the scanner and then is asked to touch the touch pad for the fingerprint scan. This allows a dual authentication with two of the traditional authentication methods involved, something the user has and something the user is. The drawback to using fingerprints as an authentication method is that the general public still has a negative association with getting fingerprints taken. There remains the perception of the criminal element.

Hand Geometry (2)

Hand geometry is very similar to the fingerprint scan described above. Hand geometry uses the characteristics of a person's hand for authentication. The main distinguishing characteristic in hand geometry is the length of an individual's finger. There are two types of hand geometry devices. They differ in the way the hand information is stored.

The first type uses a magnetic stripe card to store the identifiable information. When a user wishes to be authenticated, the card is inserted into a card reader and then places his/her hand on the sensor. The information gathered by the sensor is compared to the information downloaded from the magnetic card. If the information matches, the user is authenticated. The second type connects the sensor to a central computer, which stores the identification information. The user logs into the system either via a magnetic card or PIN number that identifies the user with his/her information. The sensor measurements are confirmed with the computer and the user is authenticated.

A couple of advantages arise from using a computer for storing the reference files. Once such advantage is that tolerance levels can be set for each individual. Each user has idiosyncrasies that can cause false positives. By setting different tolerance levels, a user who produces consistent reads from the hand geometry device can be assigned a smaller range of error. The more inconsistent users can be given a larger range of tolerance that should reduce the number of Type I errors discussed earlier.

As with most biometric authentication techniques, the performance of a hand geometry device can be degraded by changes in the user's characteristics over time. The other advantage of using a computer for the storage of the reference files is it allows for the tracking of changes in characteristic of an individual.

Signature Dynamics (3)

The signature has long been used as an identification mechanism for individuals. Signatures on checks, invoices, receipts, and even on the back of credit cards have been a primary identification tool. Using the traditional signature as a means of authenticating a user to a network has numerous drawbacks. Signatures are easy to duplicate in the traditional form and would not be any more effective than the traditional password. However, researchers have identified electrical signals are generated when a person writes their

© SANS Institute 2000 - 2005 Author retains full rights.

signature. The signals result from the varying pressures and speeds of the user's writing movements. Once the sensor has recorded the signature, the electrical signals collected are compared to that which is on file.

Voice Verification [2]
Voice verification uses a computer to analyze a users speech pattern to authenticate. A file is created for each user that contains a set of standard phrases that will be used for the authentication of the user. To authenticate, the user is asked to speak a sample of the phrases on file, the voice sample is compared to those on file and the user is authenticated. The first thought that would come to a critic's mind would be that the voice of a valid user could be recorded and used to gain unauthorized access. There are controls available to minimize this. Phrases used to authenticate a user can be randomly selected from the sample, which was recorded when the user was first defined to the system. While this doesn't completely rule out an imposter's recording being successful, it does substantially limit the possibility.

Voice verification techniques have long been used in the futuristic movies as the identification method of choice. As far as the practical implementation into the real world, voice technologies have a ways to go to become a reliable identification method. Despite the advancement in technologies and the protection against hacking attacks, voice verification has limitations which make it the most susceptible to Type I errors. A user's voice can change because of a cold or laryngitis causing a large number of errors with this technology. On a positive note, the cost of implementation of this technology could eventually be relatively small. The authentication tool used to collect the voice sample can be a simple microphone attached to the PC.

Iris/Retina Scanning [3]
Retina scanning technology uses the blood-vessel patterns of the retina to identify individuals. The retina is located on the rear portion of the eyeball. The scan is performed by lasers and requires the user to be within a couple of inches of the scanning device. The identifying information is stored in a database like all of the other biometric methods. While this method is highly effective, there are many drawbacks to the retina scanning technique. Glasses have been known to distort the readings taken by the scanning devices. There is also a public apprehension towards a laser scanning their eyes. Not to mention the equipment used to perform the scans is still very costly. For these reasons, the retina scanning method will probably not be widely used for authenticating to networks and computers anytime soon. There are a few instances where the retina scanning is being used to control physical access to buildings.

Iris pattern scanning is a similar technology to the retina pattern scanning discussed above. With iris scanning, the identifying features are the unique characteristics, which make up the colored portion of a person's eye. Again this

© SANS Institute 2000 - 2005

Author retains full rights.

technology utilizes a database to store a file containing a standard for each authorized user. Iris scanning is also a reliable technology like the retina scanning, with both providing a highly accurate authentication method. However, iris scanning is more cost effective and more widely accepted among the user community. The costs for iris scanning, while lower than retina scanning, remains too high to be cost effective as an authentication device for networks and applications. The main reason for this is that computers, to this point, have not been built with cameras as standard equipment. In the past year or so, however, we have seen the trend of digital cameras being included in most home computers packages on the market.

Face [3]

The biometric technologies noted above all provide a strong authentication control for physical access to buildings or computer rooms. Yet of the four, only the fingerprint option comes close to being capable of providing a transparent enough technology to use for the protection of data. For biometrics to be an efficient mechanism for authenticating to a computer and/or application, the technology would have to include a way of authenticating which is transparent to the user. The last thing a user wants is to stop typing or have reading interrupted at regular intervals so that they can remain connected to applications. While the fingerprint technology would probably be the most transparent of the four discussed so far, Face recognition is an option which is currently gaining ground. A small camera mounted to the computer screen can provide transparent authentication. The methods currently under development consist of a small camera attached to the corner of the computer screen. The camera is used to take a picture of the user sitting in front of the monitor. The image is then compared to the images on file, if there is a match the user is authenticated and is allowed to continue. If the user in front of the camera at the time of the scan is not a authorized user the work is saved and the applications are closed. Likewise if there is no person present at the time of the scan the computer is reverted to the screen-saver state.

Biometric Solutions

During research for this paper, I found the Biometrics Consortium at www.biometrics.org .[4] The Biometrics Consortium site also provides a lot of information on biometrics in general and on the current standards. The website also provides numerous links to providers of biometric technologies. While it is not in the scope of this paper to recommend the best biometric solution (that would depend on a number of factors, which vary between companies), let's look at a couple of vendors to get a feel for the marketplace. It is important to remember that not every solution will work for your implementation needs. A thorough evaluation of a number of products is recommended before decisions are made. Since fingerprint and face recognition technologies seem to be easiest to implement for network and application security, I will focus on a couple of companies, which specialize in these technologies.

© SANS Institute 2000 - 2005

Author retains full rights.

Authentec, Inc. (www.authentec.com) [5] provides fingerprint-scanning technology based on their TruePrint Technology. The TruePrint Technology scans beneath the surface layer of the finger to get a scan of the real fingerprint. This eliminates some of the conditions, which causes error in the fingerprint readings on most traditional systems.

Cyber-SIGN (www.cybersign.com) [6] provides signature verification technology. As we discussed earlier, the simple signature comparison does not provide an accurate authorization method. The simple signature comparison can be compromised with a bitmap image or a copy of an authorized signature. Cyber-SIGN uses dynamic signature technology to address this weakness in the signature verification arena. As described above the dynamic signature technology uses the varying speeds and pressures that are present with a person writes his signature to identify the individual. The Cyber-SIGN equipment is relatively inexpensive, using a signature pad to collect the signatures, around $100 per PC.

Limitations of Biometrics

With all of the advantages of the biometric devices, one has to wonder why is there such a delay in implementing them into our everyday lives. There are two main reasons: fear and privacy.

The Fear Factor

There is still a high level of apprehension when it comes to the general public submitting themselves to biometric identification. One of the biggest drawbacks to the iris and retina scanning technologies remains to be the public's trust in allowing a laser to scan their eyes. Lasers have traditionally been thought of a something that is used to cut holes into metal and can be harmful to ones health. This is despite the fact that there has yet to be evidence to support these fears As these technologies mature and become more common, the public's apprehension may slowly dissipate.

Privacy Violations [8]

Privacy laws have recently been enacted with the purpose of keeping sensitive customer information, such as financial and medical records confidential. For the security professional this places a renewed emphasis on data security. As mentioned before, no password alone is completely secure. With all of the vulnerabilities inherent to information systems it is only a matter of time before even a strong password can be cracked.

Even with the renewed focus on securing information to ensure compliance with privacy laws, many concerns have been raised as to the constitutionality of some biometric technologies. One such concern can be illustrated by this real case scenario: Face recognition technologies was used to capture pictures of spectators as the entered the Super Bowl stadium. The pictures were quickly compared to a database containing the images of know criminals. Over two

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

dozen arrests resulted from the use of this technology. Critics have said such surveillance was a violation of the Fourth Amendment of the United States Constitution (unreasonable search). (6)

It will be interesting to see what effect, if any, the events of September 11th will have on the recent renewed focus on privacy. We might never know if biometric technology would have prevented the horrible events of that day, but pictures of the suspected highjackers (know to have terrorist ties) were available soon after the events have taken place. In retrospect the inconvenience of a facial scan, which may even be transparent to the actual passengers, is well worth the two-minute delay in boarding a plane.

Biometric authentication technologies are meant to further secure access and thus protect the privacy of the personal information that companies collect. As we move on in the development of the biometric arena, look for more and more use of biometic technologies into our everyday lives. The more computers become a part of our everyday routine, the easier some of these technologies will be to implement. As the biometirc industry continues to grow and the need for information security continues to rise, we may see the ultimate solution to our security concerns emerge as a combination of passwords, tokens, and biometric technologies.

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

Sources

(1) Kessler, Gary, Passwords – Strengths and Weaknesses, January 1996, http://www.garykessler.net/library/password.html.

(2) Vallabhanei, S.Rao, CISSP Examination Textbooks – Volume 1: Theory, Schaumburg, SRV Professional Publications, 2000.

(3) Tipton, Harold; Krause, Micki, Information Security Handbook, Boca Raton, Auerbach, 2000.

(4) The Biometric Consortium: http://www.biometrics.org.

(5) http://www.authentec.com.

(6) http://www.cybersign.com.

(7) Woodward Jr., John, Super Bowl Surveillance – Facing Up to Biometrics, RAND, 2001, http://www.rand.org/publications/IP/IP209/.

(8) Kearns, David, Biometrics: security savior or privacy violation?, January 1996 http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci773850,00.html .

(9) www.infosecnews.com
Armstrong, Illena; Lynch Charles, Biometrics Technology - Making Moves in the Security Game, March 2002, http://www.scmagazine.com/index2.html.

© SANS Institute 2000 - 2005 Author retains full rights.