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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Scott Frazee
GSEC Practical Assignment Version 1.2e
June 29, 2001

Biometrics… Why Bother?

Introduction

With security breaches becoming more frequent and more expensive it is imperative that organizations both large and small increase their security measures. Couple this with the fact that hiring and retaining qualified IT staff is becoming more difficult and more expensive and you have an ever increasing need to administer, support and secure systems as effectively and efficiently as possible. Biometrics may be the key.

This document will provide information to consider when evaluating whether or not deploying Biometric authentication systems and associated technologies is right for your organization. Various biometric authentication methods and relevant biometric security issues will also be covered.

Definitions:

Biometrics - is the automated technique of measuring a physical characteristic or personal trait of an individual for purposes of authenticating that individual.

Authentication – is the verification of the identity of a person or process.

Why Bother with Biometrics?

Here's why…your security defenses are only as strong as the weakest link. This weakest and costly link often proves to be the human element of security. Whether it is users intentionally sharing passwords or the ease with which security information is obtained through social engineering, the more we can do as security professionals to strengthen that weakest link, the better. Consider the following information from an article posted on the Security Information Management Online Network - SIMON:

> According to CSI and the FBI, in 2000, the average loss due to sabotage of networks or data reached an estimated $535,000. Theft of proprietary information resulted in average financial losses of approximately $1.1 million. [1]
>
> Forrester Research, Inc. (http://www.forrester.com), an independent research firm, Cambridge, Mass., conducts analysis on the impact of emerging technologies. They have found that password problems account for between 40 percent to 80 percent of all IT help desk calls. According to the GartnerGroup (http://www.gartnergroup.com), a

© SANS Institute 2000 - 2002, Author retains full rights.

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

> technology research and consulting firm, Stamford, Conn., resetting forgotten or compromised passwords can cost as much as $340 per user annually. And, other estimates place the total annual cost of password administration in the range of $600 to $800 per user.[1]

Given the above statistics and considering that there are solutions that include both network software and workstation hardware at costs as low as a few hundred dollars per user, it seems obvious that there could be some significant savings available through a biometric based system.

What Biometric Authentication Methods are Available?

There are several types of Biometric authentication methods. Each has advantages and disadvantages. Some of the most common are listed below:

Fingerprint Scanning - requires the placing of your finger on a small optical scanner. Your fingerprint is quickly scanned, converted and stored digitally in a database. "Today, thanks to its relatively low price (retail units go for under $100; chips cost $20-$30), high accuracy and compactness, it's integrated into keyboards, mice, notebooks and small peripheral devices." [2] The record size for Fingerprint Scanning is between 512 and 1000 bytes. The scanned print can then be compared to other fingerprint scans for authentication. An advantage of fingerprint scanning is that it is widely accepted as a reliable means of human recognition and authentication. A disadvantage is the need for physical contact with the scanner and the public perception of fingerprinting or in this case finger scanning being associated with crime and criminal behaviors.

Retinal Scans - involves scanning of the innermost layer of the wall of the eye, the retina. The scanner emits a beam of light that reflects off the retina and returns to the scanner. The system then quickly maps the eye's blood vessel pattern and digitally stores it in a database. The record size for Retinal Scans is 35 bytes. The eye's natural reflective and absorption properties are used to map a specific portion of the retinal vascular structure. Advantages of retinal scanning include the unique characteristics of each person's retina as and the fact that the retina remains fairly stable through life. Disadvantages include the need for fairly close physical contact with the scanning device, the that any trauma to the eye and some diseases can alter the retinal vascular structure.

Iris Scanning - is based on the measurement and recognition of the colored circle that surrounds the pupil. The iris contains unique structures, which don't change with time, so no two irises are ever the same. This technique requires no physical contact and uses video technology, which quickly records the iris' unique features from about nine inches away. The system software captures the unique information from the iris and digitally stores it for later recall and authentication. The record size for Iris Scans is 256 bytes. Disadvantages of iris recognition include the expense of the systems, and problems with user acceptance.

© SANS Institute 2000 - 2002, Author retains full rights.

Hand Geometry – this non-evasive method, makes a digital three-dimensional record of the length, width and height of the hand and or thumbs and fingers. The hand is placed in an optical scanner, which takes the measurements and digitally stores the results. The record size for Hand Geometry scans is 9 bytes. While this saves on storage and speeds retrieval it also increases the likelihood of false positives unless additional unique characteristics are included in the scan. Disadvantages of Hand Geometry include the lack of uniqueness of hand geometry as compared to other biometrics. In addition, if an individual receives an injury to the hand, which causes the measurements to change, it could result in recognition problems.

Signature Verification - records biometric data present in the components of an individual's signature. The four components include the speed, pressure, style and direction. Disadvantages include problems of long-term reliability, the lack of accuracy, and cost.

Other - types of biometric methods you may want to investigate further include; Facial Recognition, Vascular Patterns, and Voice Dynamics.

Which method is best & what about reliability?

Unfortunately as with most security solutions, there is no biometric silver bullet. The unique circumstances of your situation will need to be considered. Depending on the specific application one or more biometric solutions may be ideal. If for example you are guarding Military Secrets, the length of time it takes to do a scan or multiple scans and the intrusiveness of them wouldn't be that critical to the users acceptance of the process. They pretty much don't have a choice. On the other hand if you are simply tracking time worked at a given store location you wouldn't want or necessarily need multiple intrusive biometric scans to authenticate the employees clocking in, especially if you are dealing with large numbers of employees. The time required and the intrusion level may prove unacceptable to the employees.

Along with the user component you must also consider the functionality, speed, accuracy and reliability of the systems themselves. Continuing with the Military Secrets example, accuracy and reliability would be very critical and the cost to ensure accuracy wouldn't be much of a barrier. On the other hand, if you are just trying to prevent fraudulent time tracking, accuracy would not be as critical and cost could definitely be an issue.

Regarding reliability, there are those that believe that biometrics isn't quite ready for prime time. However, an article based on Amitai Etzioni's latest book The Limits of Privacy states otherwise.

> Critics argue that biometrics are hyped and not 100% reliable. In a test conducted at the University of Georgia, in which 18,000 students were

© SANS Institute 2000 - 2002, Author retains full rights.

> screened to ensure that they did not pass their unlimited meals tickets to friends, the scanners did not recognize some 10 students. Jim Wayman, who studies these systems at San Jose State University, reports a failure rate as high as 2%.
>
> But even according to the most pessimistic assessments, biometrics defies comparison because it is much more reliable than existing modes of identification. While fooling biometrics is extremely difficult, people can buy false driver's licenses and green cards for $50 in many American towns bordering Mexico. Most college campuses are awash in false, paper-based ID cards used to purchase drinks. [3]

In addition to reliability, a systems accuracy is also a critical component to consider and is determined by the following 3 components:

Failure to Enroll rate - is the percentage of people that do not have sufficient sample quality to enroll on a given biometric system. This may be due to incorrect finger presentment, poor finger condition or problems with the biometric system.

False Rejection Rate - is the rate at which the system incorrectly rejects a legitimate attempt to verify.

False Acceptance Rate - is the rate at which the system incorrectly accepts an invalid verification attempt.

Also important to the selection process is ease of use. Regardless of how accurate a system is, the more difficult or inconvenient the system is to use, the more frustrated your users will become and the more money you will spend on training and implementation. You must also keep in mind the value of what you are trying to protect vs. the cost of protecting it.

A chart from the International Biometric Group, which is shown below, helps to draw comparisons between the most prevalent biometric technologies.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

The Zephyr Chart illustrates the comparative strengths and weaknesses of each biometric technology. The eight primary biometric technologies are listed around the outer border, and for each technology the four major evaluation criteria are ranked from outside (better) to inside (worse). [4]

Implementation Considerations

Regardless of what type of biometric technology is implemented there is much more to the overall project cost than just the cost of the capture hardware and software. When examining the cost of a biometric implementation, companies frequently focus on just the cost of the scanning or capture hardware and associated software. The reality of a biometric solution is that the actual cost of implementing any of these technologies goes far beyond hardware and software cost. It includes providing the application server hardware, the integration costs, as well as the installation, training, user research, education, marketing costs and possible initial productivity losses.

Some additional considerations or questions to ask your self as stated by Thor A. Christensen in his article, “Biometrics: Advancing Effective Security Management” are listed below:

> Does the security software support all of your operating systems?
>
> Can it apply biometrics to all of your applications without requiring modifications to application code?
>
> Does the software truly eliminate the redundancy of user names, PINs or tokens?
>
> Does it support the biometric devices that your organization may want to use today, and tomorrow? [5]

I’d like to add that the solution you choose has to not only meet the functional requirements but also your corporate culture. This is especially true when looking at widespread deployments that reach all the way to the top of the organization. If the CEO is threatened by or not comfortable with the technology then the management support needed for a corporate wide implementation will never be found.

Conclusion

Whether you are trying to reduce support costs, trying to implement single sign on or simply trying to add another layer to your Defense in Depth security strategy, biometrics should be considered. There are both advantages (you can’t lose, forget or share your biometric information) and disadvantages (hidden costs, potential legal issues and public acceptance) to biometrics. With the price of biometric hardware continuing to drop, the cost of providing IT support continuing to rise and the ability of users to remember passwords not improving anytime soon, a viable business case for biometric shouldn’t be too hard to develop assuming you can demonstrate an acceptable return on the investment. As stated previously however, each situation is unique and you must consider the value of what it is you are trying to protect and what the acceptable level of risk is for your organization.

References

1. “BioconX, Inc. Advances Computer Security Software”. Security Information Management Online Network. January 2001. URL: http://www.simon-net.com/pressRelease.asp?ID=3475 (22 June 2001)

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

2. Thieme, Michael. “Mapping Form to Function Is biometrics technology poised to become the next killer app for individual authentication?” Information Security Magazine. March 2000. URL: http://www.infosecuritymag.com/articles/march00/features1.shtml (25 June 2001).

3. Etzioni, Amitai. “Biometrics Are Coming! Biometrics Are Coming!” SpeakOut.Com Article. April 1999. URL: http://www.speakout.com/Content/ICArticle/3808 (25 June 2001).

4. "ZephyrTM Charts”. International Biometric Group. Date Unknown. URL: http://www.biometricgroup.com (26 June 2001)

5. "Biometrics: Advancing Effective Security Management." DM Review. May 2001. URL: http://www.dmreview.com/master.cfm?NavID=55&EdID=3348 (26 June 2001).

© SANS Institute 2000 - 2002, Author retains full rights.