Global Information Assurance Certification Paper

Biometrics and Password Administration

GIAC Security Leadership Certificate Practical Assignment Version 1.0

Dan Clemens
January 21, 2003

Abstract: Using Biometrics to increase network security and decrease the cost of password administration.

Definition of Biometrics Technologies: "automatic methods for the identification or identity verification of individuals using physiological or behavioral characteristics."[1]

Selection Criteria:

As the number of software applications and networked computers has increased the costs associated with password administration have risen substantially. A recent survey by Rainbow Technologies noted that the average network user has to remember five-and-a-half passwords.[2] This often leads to one of four situations: the employee selects one password and uses it for all applications, passwords are written down, easy-to-guess passwords are used, or passwords are forgotten and the help desk is called. The end result of poor choices by network users is decreased security or increased costs.

One possible solution to improve security while decreasing the overall cost of password administration is through the use of biometrics. By utilizing biometrics, the need for employees to use passwords is greatly reduced, or in some cases, almost eliminated. Employees will no longer be able to forget their passwords or resort to writing them down. Additionally, employees will not be able to accidentally or intentionally give out their biometric characteristic or trait, as with passwords.

Impact on Business:

Increased network security has become even more important in light of recent legislation passed by both Federal and State governments. Companies now must comply with the Health Insurance Privacy and Portability Act, the Gramm Leach Bliley Act and in some cases the state of California's recent disclosure law. Each regulation or law carries civil and even criminal penalties ranging from monetary penalties up to $1,000,000.00 in addition to criminal charges that carry a penalty of up to 10 years in federal prison.[3] The business will still be faced with how to restore its damaged reputation and the resulting loss of customers.

The cost in terms of lost productivity due to employees forgetting a password can also be very expensive to a company. According to one estimate, password

---

[1] Nuger, Kenneth, Phd. "Biometric Applications: Legal and Societal Considerations" Original presentation date unknown. http://www.engr.sjsu.edu/biometrics/publications_consideration.html (10 Dec. 2003)
[2] Rainbow Technologies. "Rainbow Technologies Survey: Passwords Are Insecure and Costly; Pose Significant Security Risk for Corporate Data" 6 Aug 2003 http://www.itsecurity.com/tecsnew/aug2003/aud47.htm (10 Jan 2004)
[3] Unknown Author, Kent Trust Security Solutions, "Gramm-Leach-Bliley: What does it Mean for You" Original publication date unknown. http://www.kenttrust.com/Kent_GLBA_Whitepaper.pdf (21 Jan 2004)

related calls are made on average of four times a year per end user and cost anywhere from $51 to $147 per reset.[4] Even for a midsized company with 2500 end users, this can cost anywhere from $127,500 to $367,000 per year in lost productivity.[5]

Challenges:
While each type of biometric device has unique challenges, each device will also share a set of common challenges in the areas of implementation and error types.

All biometric devices must be implemented prior to being used to reduce the use of passwords. The implementation process will involve having network personnel or a local technician install hardware and software. The next step will be to enroll the users into the system. During enrollment the user will have their biometric data scanned to create a template. A template is a digital representation of selected biometric data points (where fingerprint ridges end or begin, Iris or Retina patterns, etc). The template will then be compared to future scans of the individual's biometric data to verify or identify the individual. It is critical to plan for the initial identification of the user. A biometric device only matches submitted information for comparison against an established template. If an unauthorized individual were to pose as a legitimate user during the enrollment process, they would have the same network access as the impersonated employee.

All Biometric devices are subject to the following types of errors: **F**ailure **T**o **A**ccept, **F**ailure **T**o **R**eject, **C**rossover **E**rror **R**ate and **F**ailure **T**o **E**nroll.

Failure To Accept (**FTA**) happens when the system rejects an authorized user.[6]

Failure To Reject (**FTR**) happens when the system accepts an unauthorized individual as that of an authorized user.[7]

Crossover Error Rate (**CER**) is the error rate at which the FTA and FTR are equal, meaning that an equal percentage of users will be erroneously rejected while unauthorized individuals are accepted as legitimate users.[8]

Failure to Enroll (**FTE**) happens when a person can not be enrolled due to the lack of biometric characteristic's being scanned by the device (i.e. lack of fingerprints, unable to speak, physical injury to the iris or retina).[9]

---

[4] Unknown Author. "From Password Synchronization to User Identity – The Evolution of Password Synchronization and Password Reset Products" A "Blockade Viewpoint" Article May 2002 http://www.blockade.com/news/articles/ar_05_01_2002.html (30 Dec 2003)
[5] Ibid
[6] Chirillo, John, Blaul, Scott. Implementing Biometric Security Indianapolis Wiley Publications, 2003. 91
[7] Ibid
[8] Ibid
[9] Ibid

Each type of biometric device will need evaluation based on cost, user acceptance, and even on where the device will be used. As we have seen, the average cost of resetting passwords on an annual basis can be excessive. However, the actual costs to the business should be calculated based on the number of password reset calls made to the help desk on an annual basis, average time spent per call, and average salary of both the end users and help desk employees. User acceptance will also be a deciding factor in determining if the implementation of a biometric device will be successful. If users have reservations or outright objections to the use of the biometric device, implementation will not be successful. Reservations or objections will depend on how the device captures the user's biometric information. Devices that require physical contact may cause some individuals that fear the spread of germs to resist their use. Likewise, devices that scan the user's eye may cause objections if the user fears that the device may cause physical injury. Devices that do not require direct interaction with the user may be resisted if employees feel that their actions could be monitored without their knowledge. Finally, where the device is used must also be considered. If employees are required to wear protective gear (goggles, gloves, hoods, etc.) that covers the body part to be scanned, the device will not be able to function as intended. In the case of voice recognition, the level of background noise must be factored in to the decision. Areas with high levels of background noise (runways, restaurants, freeways, etc.) could drown out the user.

Policies and Legal Issues:

New policies and legal issues to be addressed will include the storage of the biometric data itself, how the data will used, sharing or selling of data, and what will happen if the data is compromised. Policies and Procedures will also need to consider how to deal with users who are consistently rejected or can not be enrolled.

Some individuals believe that an exact copy of their biometric data is created and have fears that it could be used without their permission. Additionally, depending on how the biometric device is to be used, data may be stored in a network database on the biometric device itself or even on a smart card or similar device. If users need to log on to the network from various locations, the data will need to be stored on the network or smart card. This will give the user the advantage of being able to log on from multiple workstations without having to be enrolled at each machine. However, this option will require that a database be administered or that users be allowed to possess smart cards that can be lost. If the end user needs to log on to only one workstation, having the data stored on the device or workstation can also be considered. Each option on how the data is stored will cause some users concern. If the data is stored in a central database some users will be concerned about the database being compromised. If the data is stored on a smart card, users may be concerned that someone could find the

card and have their personal information. Educating users on how the data is stored, and what safeguards are in place (only selected biometric information used, encryption of data, safer networks, etc.), can help overcome this concern.

Companies will need to decide if the data collected will be shared or sold to other businesses, individuals, or government agencies. The decision to share or sell biometric data will have a large affect on user acceptance if they feel their privacy or identity could be compromised. Prior to any decision, each company should consult competent legal counsel to weight the potential legal implications

A policy will need to address exactly how the data may be used. Will the information be used solely to authenticate users logging on to the network or can it be used to track the employee's whereabouts or actions?

An incident response program and policy will also need to be in place in the event that the biometric data is compromised. Unlike passwords that can be changed, an individual can not be issued a new set of fingerprints or retina.

Additionally users who fail to enroll or are falsely rejected on a consistent basis will need to have an alternative method for accessing the network.

EXECUTIVE SUMMARY

Definition of Biometrics Technologies: "automatic methods for the identification or identity verification of individuals using physiological or behavioral characteristics."[10]

Increased security can be achieved through the proper use of biometrics because biometric information can not be easily guessed (as with weak passwords) and users can not give away or share their biometrics information.

Decreased administration costs can be achieved through the elimination of passwords, thereby greatly reducing the time users spend tying up the organization's help desk.

The type of biometric device must be used in the appropriate setting. A scanning device will not work if the employee is required to wear protective gear over the area to be scanned, i.e. heavy gloves, hoods, dark goggles.

Biometric devices will not work for every user; some individuals lack enough of the unique physical characteristics for the equipment to work (worn fingerprints, born mute, physical damage to the body).

[10] Nuger, Kenneth, Phd. "Biometric Applications: Legal and Societal Considerations" Original presentation date unknown. http://www.engr.sjsu.edu/biometrics/publications_consideration.html (10 Dec. 2003)

All devices will have some type of error rate that will allow unauthorized users access, while rejecting legitimate users.

Policies concerning privacy and use of biometric data must be in place to address privacy concerns of the users.

End users need to be educated on the privacy and use policies to increase the acceptance of biometrics.

References:

Nuger, Kenneth, PhD. “Biometric Applications: Legal and Societal Considerations” Original presentation date unknown. http://www.engr.sjsu.edu/biometrics/publications_consideration.html (10 Dec. 2003)

Unknown Author, Rainbow Technologies. “Rainbow Technologies Survey: Passwords Are Insecure and Costly; Pose Significant Security Risk for Corporate Data” 6 Aug 2003 http://www.itsecurity.com/tecsnew/aug2003/aud47.htm (10 Jan 2004)

Unknown Author, Kent Trust Security Solutions, “Gramm-Leach-Bliley: What does it Mean for You” Original publication date unknown.

Unknown Author. “From Password Synchronization to User Identity – The Evolution of Password Synchronization and Password Reset Products” A “Blockade Viewpoint” Article (May 2002) http://www.blockade.com/news/articles/ar_05_01_2002.html (30 Dec 2003)

Chirillo, John, Blaul, Scott. Implementing Biometric Security Indianapolis Wiley Publications, 2003. 91http://www.kenttrust.com/Kent_GLBA_Whitepaper.pdf (21 Jan 2004)

Unknown Author, Drake Enterprises, http://www.drake-ent.com/hippa.htm (12 Jan 2004)

Ott, Sam. “Computer Intrusion Disclosures Mandated by New Law” (20 Nov 2002) http://www.bankersonline.com/cgi-bin/printview/printview/pl (10 Dec 2003)

Brant, Andrew. “Privacy Watch: California Law Protects Us All From Security Breaches” (Oct 2003) http://www.pcworld.com/resource/printable/article/0,aid,112023,00.asp (10 Dec 2003)