Global Information Assurance Certification Paper

Biometric Security: Not Just Fantasy

David Levin

March 6, 2001

GSEC Practical Assignment v1.2c

Introduction

Passwords are a necessary evil. They safeguard our information but, at the same time, they can be easily hacked and are quite annoying. What other options are there? How do we really know who is on the other end? With this in mind comes Biometrics. Biometrics are unique physical or behavioral characteristics of an individual, which can be measured (and thus compared). Some types of biometrics are fingerprint, voiceprint (speaker verification), facial features, iris recognition, hand geometry, and dynamic signature verification. Because biometrics are tightly bound to an individual, they can't be shared, lost, stolen, forgotten, guessed, written down, or easily hacked. If Biometrics offers such considerable benefits, why then are so many not using it? We all suspected that this technology was around the corner but it's taken quite some time to get there. This document offers advice on handling the obstacles and challenges many businesses will encounter along the way.

In the security industry, biometrics are regarded as providing the highest level of security. The methods for verifying an individual's identity are commonly broken down into the following three stages:

Stage 1 (lowest level of security) — *something you have*, such as a photo ID.

Stage 2 (second level of security) — *something you know*, such as a password to access a computer or a personal identification number (PIN) to access funds at an ATM.

Stage 3 (highest level of security) — *something you do or something you are*, which comprises physiological and/or behavioral biometrics, including fingerprints, voiceprints, signatures, etc.

Security systems can be built up using one, two, or all three of these stages, providing several levels of security. For example, you could use a card key to access your place of work, but would also be required to verify your fingerprints against the biometric stored on the card. This would ensure that someone couldn't just steal your card and gain access to your office. You could do away with the card altogether and just identify yourself using your fingerprints. Besides being easier to use, there is no physical object to lose.

Do you really need Biometrics?

According to a 1999 study, financial losses due to computer security breaches grew to over $1 billion in 1998(Computer Security Institute). Estimated cost of fraudulent schemes in the USA using false IDs is $30 billion (New York Cyber Times). 50% of help desk time is taken up dealing with password issues and password support alone costs companies up to $160 per user, per year (Network Management Magazine).

Figure 1 describes the process involved in using a biometric system for security.

Figure 1. How a biometric system works.
(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

Reasons for implementing biometrics include:

- When fraud is a problem, many computer security breaches come from within an organization where the firewall cannot provide protection.
- When you need to add a layer of physical access control to an information security system.
- When you want to reduce IT support costs.
- To protect against hardware theft.

Let's use ETrade for example, late last year they had released a more secure version of the software it uses to store passwords after learning that it had been leaving accounts vulnerable to access by outsiders. The online brokerage stores information about customer passwords in cookies, which are stored on customers' computers. The password information was protected by a scrambling technique that proved to be a weak form of security. But the vulnerable cookie wasn't the only problem. ETrade's Web site also is susceptible to what's called a "cross-site scripting attack," where an attacker could create a Web link allowing access to the cookie and the passwords it contains if an ETrade customer were to click on that link. The links could then be sent to target victims in e-

mail or could be hidden on Web sites. This is a perfect example of how biometrics can help prevent such issues as this one. Again, passwords are a necessary evil.

Which application is right for your business?

We will now look at what applications are currently available for your type of business. There are a number of different biometric applications and it's important to compare the benefits and pitfalls of each according to your business.

Following is a brief overview of some of the major options:

- Fingerprint recognition systems have a high accuracy rating, are quick to use, take up little space and are relatively low cost, so they're useful for providing security for large numbers of users. They're not suitable for employees who have to wear gloves and because they require the user's interaction, can't be used in situations where security needs to be unobtrusive.

- Voice Recognition systems are the least expensive to implement, mainly because they use a standard telephone or microphone to record a user's voice, making them ideal for large call centers. However, they require some time to learn the user's voice, and may not be as accurate as other biometric devices. The voice is also the easiest biometric feature to replicate, as hardware to record and play back speech is easily accessible. Most voice recognition systems deal with this type of threat by having a number of stored passwords and asking the user to supply one or more at random within a short period of time.

- Facial Recognition systems are one of the latest biometric devices to be developed. Typically seen in the industry as the 'holy grail' of biometrics, they're comparatively expensive due to the cost of cameras. However, they're unobtrusive and require no user interaction so they're ideal for site access control and covert monitoring. Two-dimensional facial recognition is typically easier to fool, but the latest three-dimensional systems offer higher accuracy levels and greater flexibility.

- Retina recognition systems provide high accuracy and offer the lowest risk of fraud. However, they're extremely intrusive and they require the user to place his or her eye close to a camera. As a result, they're unsuitable for the majority if corporate environments. Also, retina patterns can change during the individual's lifetime.

- Iris recognition systems provide high accuracy, but currently require camera technology which can be both expensive and bulky, making mobile use or high volume rollout an issue.

Table 1. Comparison of biometrics

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

*The large number of factors involved makes a simple cost comparison impractical.

Once you've decided which biometric type is most suited to your organization's needs, you need to go through a number of steps before choosing the specific application.

First, consider where your business needs biometric security. Is it to be used for physical security or information security? Is the aim to protect against internal or external threats? Will it apply to customers and suppliers or just employees?

Second, establish the level of security required. You can do this by measuring the effectiveness of your existing security application and then setting targets for the biometric system. This will help you evaluate potential applications.

Third, select the specific hardware device and decide on the manufacturer.

Risks and Challenges

Does it offer return on investment?

There is little analysis currently available. Factors worth considering are the existing costs of fraud and theft in your organization, costs of lost productivity from forgotten passwords, and ongoing costs required to allocate, set up and maintain password or card protected systems.

Is it a 'here today, gone tomorrow' technology?

Biometric technology itself isn't new, some categories having been around for about thirty years. The National Fraud Centre in the US has put its weight behind biometrics and the Office of Law Enforcement Technology Commercialisation has commissioned a large-scale investigation into the global biometrics market. With players like Microsoft backing the market, the future looks fairly safe. Growing subscription to standards such as the BioAPI open standard will ensure that you are not locked into any one software or hardware supplier.

Will it impact the users?

Providing users are educated about the system and it's benefits, there should be minimal impact. It may be necessary to pull in the help of the human resources department during the roll out phase, or to work with a team made up of departmental heads.

What are the legal implications?

The main legal issue is data protection. Fears have been expressed about companies selling on biometric data. This is more of a threat in the US, where there is no federal legislation protecting an individual's data. In Europe, data protection laws have been forbidden organizations from circulating personal data since March 1, 2000. As with any emerging issue as yet untested by civil law, it's vital to treat all biometric data as extremely sensitive and personal. By the same token, the Data Protection Act clearly states that companies will be liable for loss of data unless they are seen to be taken adequate measures to protect that data.

Conclusion

For many companies, biometric systems are the perfect answer to the expensive and time-consuming problems of fraud, theft, and access control. Technical and financial considerations aside, biometrics can pose a significant cultural challenge and introducing fingerprint scanners to every desktop or a facial recognition entry system has to be done sensitively. Consider how such an implementation will impact various sections of the company and plan carefully to head off potential issues before they occur.

Once the exclusive preserve of James Bond movies, biometrics now has to be considered one of the many challenges of modern management.

References

Avanti "The Biometric White Paper" Jan 2000
URL:http://homepage.ntlworld.com/avanti/whitepaper.htm (26 Mar. 2001)

IEE Computer Society "A Practical Guide to Biometric Security Technology" Feb 2000
URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (26 Mar. 2001).

Avanti "Specifying Biometrics" Jan 2000
URL:http://homepage.ntlworld.com/avanti/specifying.html (26 Mar. 2001)

PC Magazine "Biometrics and Random Computing" Dec 2000
URL: http://www.zdnet.com/pcmag/stories/opinions/0,7802,2666439,00.html(29 Mar. 2001).

PC Magazine "Biocentric Security" Jan 2001
URL: http://www.zdnet.com/pcmag/stories/reviews/0,4161,2675362,00.html(29 Mar. 2001).

Network World "Biometrics Eyes the Enterprise " May 2000
URL:http://www.nwfusion/research/2000/0508feat2.html (26 Mar. 2001)