Global Information Assurance Certification Paper

Tricia Olsson
GSEC Practical
Version 1.4b, Option 1
August 26, 2003

Strengthening Authentication with Biometric Technology

Abstract

One of the fastest growing crimes in America today is identity theft. Providing data confidentiality and integrity is vital if businesses want to combat this growing epidemic. This paper will look at the danger and cost of identity theft, uncover the problem with current authentication practices, demonstrate how a biometric solution can be used to provide stronger authentication, and look at the added benefit of using multiple factor authentication practices.

Identity Theft

Identity theft happens when criminals steal someone's personal or financial information such as their social security number, driver's license number, credit card number, or bank account number. This stolen information is used to illegally obtain loans or open lines of credit in the victim's name.

Recent Gartner reports indicate that 3.4% of US consumers were victims of identity theft during the 12 month period ending in June 2003. That percentage represents 7 million adults and is up from 1.9% in February 2002 [1]. More than 20% of all cases involve telecommunications and the Internet [3]. Additional Gartner studies show that up to 1.14% of total annual online sales were lost to fraud. For 2001 this amounted to more that $700 million in online fraud alone. Who says crime doesn't pay [2]?

For the criminal, identity theft is a high-reward, low-risk crime. Many financial institutions (credit card issuers, banks, cell phone service providers, financial service providers) do not recognize identity theft for what it is. They mistakenly write the cost off as credit losses instead of reporting the theft and prosecuting. Due to this misclassification, the criminal has about a one in 700 chance of getting caught by the authorities [1]. It's easy to see how people can be tempted into a life of crime.

Many people feel that legislators and industry associations need to apply pressure to financial institutions to provide them with sufficient incentive to recognize the crime for what it is and implement solutions that will turn the tide on this growing epidemic. Efforts like the U.S. Fair Credit Reporting Act will cover security and accuracy of personal financial information as well as access to credit and financial services [1]. A recent California law (SB 1386) will require companies to notify their California customers if their personal information is

compromised [3]. It is important that financial institutions take proper measures to prevent the practice of extending wrongful credit to identity thieves or ultimately the consumer will continue to pay the price for these crimes.

Current authentication practices

Authentication refers to the verification that you are who you say you are. For example, if you were trying to log onto a network or perform an on-line transaction, the authentication process will try to verify that it is really you. This will be done by providing the system with a characteristic or combination of characteristics that are associated with your identity. Many security services are dependant on authenticating users such as generation of accurate audit trails, non-repudiation in communications, and preserving confidentiality [19].

The three authentication methods, or categories of characteristics used today are:

- *Something you know* – a password, PIN, or personal information such as your mother's maiden name.
- *Something you have* – an ATM card, credit card, driver's license, smartcard, PKI, or token.
- *Something you are* – a unique personal trait such as a fingerprint, signature, or voiceprint [6].

Typically you incorporate a combination of these characteristics to create an authentication system. You have your ATM card and a PIN, your signature is used with your credit card, and you often confirm identity with a question/response for telephone transactions along with your account number. Using a combination of these three methods for authentication is a practice commonly referred to as multiple factor authentication. Defense in depth and layering levels of security provides the strongest authentication systems. With the growing threat of identity theft and fraud it is important to ensure data integrity and the safety of the customer's personal information.

In order to understand the vulnerabilities in current authentication practices, let's look at how they are being compromised today. An identity thief can use many different methods to obtain your personal information. These methods include:

- Finding the information in your trash (dumpster diving)
- Watching as you type your personal information (shoulder surfing)
- Stealing your mail
- Stealing or finding wallets or purses
- Overhearing conversations made on cell phones
- Intercepting faxes and emails (either in electronic or paper form)
- Hacking into computers

- Telephone or email scams (social engineering)
- Careless online shopping and banking practices

With these criminal behaviors in mind, let's take a look at some of the problems with common authentication practices in use today.

Things you have can be lost or stolen
ATM cards, credit cards, your driver's license, and items falling into this authentication method can be lost or stolen. As mentioned above, an identify thief can find your account numbers or cards in many ways and use them to their advantage. Systems using things you have for authentication must take into account the chance of the card or account number being lost or stolen.

Things you know can be discovered, predicted, or hacked
Passwords, PINs, and personal information rely on the user to make it strong and keep it safe. Strong password requirements can be imposed on the user but if the password is too difficult, the user may write the password down in an effort not to forget it. Without imposing some strength or password requirements, users may create a password that is easy to remember or predictable. This makes the job of hackers and password cracking technologies very easy. Many people reuse the same password for many different logons. If one logon password is compromised, they are all vulnerable. There is a possibility that someone could create a file on their computer with a list of their account logon IDs and passwords to keep them straight. The user may also keep a copy of confirmation emails with account numbers and passwords in an unencrypted state on their computer. If their computer is hacked, they have handed over their accounts to strangers. Personal information is often predicable or easy to find. And disturbingly, the thief may be someone you know who has easy access to your personal history or account information. It is estimated that more than half of all documented identity theft is committed by criminals that have established relationships with their victims, such as family, co-workers, roommates, or neighbors [4].

Something you are often relies on manual verification
A sales clerk looks at the signature on the back of your credit card and compares it to your actual signature. A bouncer at a bar looks at the date of birth on your driver's license and uses your picture to verify that it is your license that is being used. Many verification methods in use today rely on manual processes. These manual efforts are very susceptible to error. They are easily missed or forgotten in the rush to provide good customer service and may be easy to forge or impersonate. There is however a more reliable form of this authentication method that can be used, a biometric.

What is a Biometric?

A biometric is an automated method of recognizing an individual based on physical or behavioral characteristics. Physical biometrics measure many unique characteristics of a part of the human body to create a print or template. Common physical biometrics include fingerprints; hand or palm geometry; retina and iris recognition; or facial characteristics. Examples of behavioral biometrics include signature, voice, or gait recognition; and are based on indirect measurements of the body (things we do that are unique to us). Generally, physical biometrics are more accurate than behavioral biometrics.

Let's look at a brief summary of some of the common biometric types:

Fingerprint	Looks at the patterns found on the fingertip including location and direction of ridge endings and bifurcations.
Hand Geometry	Analyzes and measures the shape of the hand including height and width of bones and joints in the hands and fingers.
Retina	Analyzes the layer of blood vessels in the back of the eye.
Iris	Measures furrows and striations found in the colored ring of tissue that surrounds the pupil.
Facial	Analyzes and measures facial characteristics. Common feature extractions are position and shape of nose and position of cheekbones.
Voice	Voice patterns (frequency, duration, and cadence) are transformed into text for a voice-to-print match.
Signature	Signature features such as speed, velocity, and pressure are analyzed to create this unique print.

Biometric-based authentication is considerably more accurate than current methods. It links the verification process to an individual not to a card, account number, PIN, or password. A biometric cannot be shared, forgotten, or lost. The process is automated instead of relying on manual verification.

Biometrics come is a wide range of accuracy, reliability, and usability. For example, the retina and iris scan are considered among the most accurate and unique biometric options. However, proper training is a key component because during the scanning process the user must be positioned correctly in front of the scanner, glasses must be removed, and proper lighting is required. Cost of the eye scanning device is also a consideration. The cost of an iris scanning devices is considerably higher than say, that of a fingerprint scanner. A fingerprint biometric is easy to use but requires physical contact with the scanning device and can potentially be contaminated by something as simple as the person before you using too much hand cream, thus smearing the reader device.

A Biometric Authentication System

When creating a biometric solution it is important to understand the distinction between authentication and identification. During identification the system takes the live biometric sample and attempts to find out who it belongs to by comparing it to a database, or store of biometric templates to locate a match. This is a one-to-many comparison. Conversely, an authentication system is a one-to-one search. The live biometric sample is compared to a stored sample previously given by that individual, and the match confirmed. In this instance, the biometric is not required to be stored in a central location. A one-to-one match saves processing time and computer resources over the one-to-many comparison since it does not need to compare the live scan to the entire database for a match. The ability to store the biometric template outside of a central repository, perhaps in a smartcard, also has advantages when looking at privacy and performance concerns. The biometric can now be placed back in the hands of the user not in a database outside of their control.

In order to use a biometric for authentication it needs to be part of a biometric system. A biometric system converts the data which has been recorded from the chosen physical or behavioral characteristic into a biometric template. This template is used to compare against a live biometric sample to determine if it is a match. The steps involved in a biometric system are:

1. Capturing the chosen biometric. This is sometimes referred to as the enrollment process where a user's initial biometric sample is collected.

2. Process and extract the biometric template. This is the automated process of encoding the distinctive characteristics of the biometric sample to create a biometric template. Processing is done to locate a sufficient amount of accurate data. The algorithms used to extract features and create the template will vary from vendor to vendor.

3. Store the template. The template can be stored anywhere from a central repository to a portable token or smartcard.

4. Live-scan the biometric. Hardware devices to read the biometric print (cameras, scanners, microphones) come in many shapes, sizes and price ranges. Some are easy to use such as talking into a microphone or telephone, while others require special lighting or positioning in order to obtain the print.

5. Extract the biometric template from the live scan. As in step 2 above, the biometric template is created by processing the data.

6. Match the scanned template against the stored template. As stated earlier this could be in a central repository, a data store within the scanning device or a portable media like a smartcard.

7. Provide a matching score back to the application. It is fairly safe to say that no two templates of the same biometric will match 100% of the characteristics 100% of the time. Reliability or quality of a scan will cause the result to vary. This can happen for a number of reasons; the scanner may be dirty, a different type of hardware devices is used, your position is not quite right, or the lighting may be off. It is also possible for some of your characteristics to change, such as a burn, scar, or even a head cold. In order to allow for this variance a score is used to determine if the templates have enough matching characteristics to be considered the same print.

8. Record a secure audit trail. Any good security analyst can tell you the importance of an accurate audit trail. Audits, investigations, and trend analysis all rely on good auditing practices.

Accuracy of a biometric system

A biometric solution is not the authentication silver bullet. Measures must be taken to ensure the identity of the person when the biometric template is originally stored. If anyone can say they are me and store a biometric in my name, then we've just given the criminal a secure way to steal my identity. There are factors that will cause the biometric template to vary between one scan and the next. This could be caused by the scanning device used, environmental influences, or changes the biometric itself (such as a scar, sore throat, or a broken nose).

As we touched upon earlier, when a stored template is compared to a live sample a score is given back to the application based on the number of characteristic or feature matches. What constitutes a passing score can be adjusted. The score can be set very high to provide a very secure system or it can be lowered to allow for variance and increase user convenience. If the score is set too high, the chance of a valid sample being rejected is greater. The term for this occurrence is a false rejection rate, or FFR. On the other hand, if the score is set too low, the chance of an invalid sample being accepted is higher. This is known as a false acceptance rate, or FAR.

Many reports have been written on the psychology of biometrics. One of the big concerns is user acceptance. If a person cannot count on consistency in the access and is commonly rejected when making a valid entry attempt, user confidence is lost. Not to mention the stigma and frustration that goes along with being rejected. Nobody wants that. It is important to find the right balance between FFR and FAR. The system needs to provide a sufficient level of security as well as provide usability and user acceptance.

Measurements can be taken to estimate system accuracy. FFR and FAR rates are interdependent and can be plotted against each other to determine the crossover error rate (the point at which FAR and FFR are equal). The lower the crossover error rate, the more accurate the authentication will be.

Many questions must be answered when designing a biometric solution. The overall vulnerability of a biometric system is derived from several areas of risk. A thorough risk assessment should be completed before any new authentication system is implemented. Here are some of the questions to consider in your risk assessment:

- What methods of validation are used when the initial biometric sample is created?
- What are the physical attributes of the user facing device? Is it tamper resistant or have a reporting mechanism?
- What is the connectivity between authentication points? Are third party networks secure?
- Are all back end interfaces and host controller processes secured?
- How fool proof is the biometric scanning device?
- Are there any overwriting vulnerabilities? For example, can the user opt to use a password instead of the biometric?

Third party biometric solutions offer a wide variety of algorithms and measurements to create the biometric template. Additional considerations when evaluating a biometric solution should include; the level of security needed, level of accuracy required, performance, feasibility of implementation, stability of the technology, vendor credentials, cost of implementation, user acceptance rate, size of the template, and what other layers of security or authentication will be used.

Standardization in Biometric Technology

The biometric industry business is a booming. There are more than 150 separate hardware and software vendors, each with their own algorithms and means to extract and create the biometric template. The acceptance of a new technology goes hand in hand with standardization of its central functions, formats, and processes. The development of industry standards defines common methods to interface with a biometric application as well as provide an effective way to evaluate and compare biometric technologies.

One of the most common biometric standards is BioAPI which defines an open system standard application programming interface (API) allowing applications to interface with biometric technologies in a common way. Another important standard is the Common Biometric Exchange Framework Format (CBEFF) which allows applications to recognize information like device type, version number and vendor name, without additional software [18].

One area not fully addressed by a standard is the way matching accuracy (FAR and FFR) are gathered and reported. There is however the Best Practices in Testing and Reporting Performance which has become widely adopted [18]. These best practices control some of the variables in biometric measurement and reporting.

Biometrics as Part of a Multifactor Authentication Solution

Using biometrics as part of a multifactor authentication systems is a method of combining one biometric technology (something you are) with other authentication methods, such as a smartcard (something you have) or a password (something you know). When you combine technologies you now have additional security factors working in tandem so the need for the highest-level FAR may no longer be necessary. You now have a second means of verification to help prove the authentication.

One possible multifactor authentication solution would combine biometric verification with VPN over the internet. A VPN connection provides secure and encrypted communication, while the biometric could provide a higher level of confidence as to the user's true identity. While the availability of devices may make this a reasonable solution, implementation would be a major undertaking [9]. Adding authentication that requires the addition of hardware and software in every home is a challenge. While there are several industry standards in place, many questions of interoperability have not yet been addressed. Can the biometric device be something already in every users home (perhaps a microphone for a voice authentication)? Will there be additional costs for the end user? Will the user have confidence and acceptance of the solution? Use of a biometric in an internet scenario is good in theory, but may not be ready for prime time yet. But will the assessment be the same 3 years from now? Look how far biometrics have come in the past 3 years.

Another multifactor authentication combination would add biometrics to an existing system. For example, biometric readers that work with existing keypad, proximity, and magnetic stripe card readers are available. This solution would typically use the biometric as a buffer for the pre-existing access identification after successful validation of the biometric template [14]. This is an attractive option for perimeter access where proximity-based access control is in place. The normal proximity access can be used for primary access control, but the biometric would control access to higher level secured areas using the same card.

Smartcards combined with a biometric offer a number of advantages. A smartcard offers portability for the biometric template. Providing the template at the biometric device removes any storage limitation on the device or access to a central repository. A smartcard offers a certain level of tamper resistance since

the chip is embedded and sensitive data can be encrypted. As smartcard and biometric technology mature, we can anticipate more opportunity for multifactor solutions combining these technologies. Smartcard enhancements promise to deliver more processing power, more memory, faster transfer rates, and lower costs. When greater interoperability becomes available, the flood gates will open for large scale deployments. There is already interest from some governments to introduce an ID card which would use smartcard technology combined with a biometric.

My personal favorite multifactor authentication solution combines biometrics with smartcards and public-key infrastructure (PKI). You still get the advantage of the portable biometric template with the smartcard, but you add an extra layer of security with cryptography. PKI is mathematically more secure than biometrics and it can be used over the internet. The main flaw in PKI is the security of the user's private key. That's where the biometric comes into play. The private key can be stored on the smartcard and protected with the biometric. This offers one of the strongest authentication combinations, but as with any solution must be measured against the feasibility and costs.

Future Applications

Let's take a minute to look at the possibilities. What could our World be like if we used biometric authentication in our everyday lives?

I envision a World where there are no waiting lines in airports. My passport is a smartcard with biometric templates of my fingerprint and facial scan. All I need to do is walk up to the gate, insert my passport, offer my finger to a scanner, then smile for the camera and I'm on my way (notice I included two forms of biometrics for stronger authentication).

When I need money from the bank, all I need to do is offer my fingerprint instead of remembering a PIN at the ATM. But why use cash at all? I never need to sign for a credit card or remember my PIN for my debit card, just swipe, touch the scanning device, and off I go. And let's remove the long wait in checkout lines? Just scan the items you are purchasing, swipe, touch and go. How much easier can it get to spend your hard earned money?

As I walk up to my computer in the morning at work it automatically logs on and greets me with a friendly hello (using a facial recognition and proximity ID badge of course). And it goes without saying that I had instant access to the building when my gait was recognized as I walked up to the door and validated using the same proximity ID badge (which is a smartcard). What a pleasant way to start the working day, doors are opened for me and I am always greeted with a pleasant good morning.

Sound too far fetched? Maybe they're not quite feasible yet; but the technology is there and these solutions are more than just possible, but in my opinion probable. Just give the technology some time to grow and mature.

Conclusion

One of the fastest growing crimes in America today is identity theft. We have shown that providing data confidentiality is vital if businesses want to combat this growing epidemic. If financial institutions do not take measures to ensure data integrity; legislators and industry associations may step in to apply pressure and pass laws to force the change.

Authentication practices in use today have vulnerabilities. This paper identified how each of the three authentication methods have flaws. We discovered how a biometric solution can automate the verification process and provide a method of verification that cannot be lost, shared, or forgotten.

And finally, we demonstrated how using multiple factor authentication including biometric technology can provide some of the strongest, if not yet feasible, solutions available. Biometric authentication can no longer be considered a futuristic option. Many solutions are in practice today and we may soon start to see large implementations that can impact our everyday lives.

References

[1] Gartner Group. "Gartner Says Identity Theft Is Up Nearly 80 Percent." 2003 Press Release. URL: http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp (7/25/2003)

[2] Gartner Group. "GartnerG2 Says 2001 Online Fraud Losses Were 19 Times as High as Offline Fraud Losses." 2002 Press Release. URL: http://www3.gartner.com/5_about/press_releases/2002_03/pr20020304c.jsp (7/25/2003)

[3] Litan, Avivah. "Stolen Credit Card Case Should Prompt Card Companies to Act." 20 February 2003. URL: http://www3.gartner.com/DisplayDocument?id=386665&ref=g_search (7/25/2003)

[4] Jaques, Robert. "Identity Theft Rockets 80 Per cent." 23 July 2003. URL: http://www.vnunet.com/News/1142517 (7/25/2003)

[5] "Identity Theft Prevention and Survival." URL: http://www.identitytheft.org/ (7/25/2003)

[6] Liu, Simon & Silverman, Mark. "A Practical Guide to Biometric Security Technology." URL: http://www.computer.org/itpro/homepage/jan_feb/security3.htm (4/14/2003).

[7] Ashbourn, Julian. "Vulnerability with Regard to Biometric Systems." 2000. URL: http://homepage.ntlworld.com/avanti/vulnerable.htm (6/17/2003).

[8] Ashbourn, Julian. "Remote Network Access." 2001. URL: http://homepage.ntlworld.com/avanti/remoteaccess.htm (6/17/2003).

[9] Ashbourn, Julian. "Biometrics and The Internet" 2000. URL: http://homepage.ntlworld.com/avanti/internet.htm (6/17/2003).

[10] Ashbourn, Julian. "Smartcards Synopsis." 2002. URL: http://homepage.ntlworld.com/avanti/smartcards.htm (6/17/2003).

[11] Ashbourn, Julian. "User Psychology and Biometric Systems Performance." 2000. URL: http://homepage.ntlworld.com/avanti/psychology.htm (6/17/2003).

[12] Ashbourn, Julian. "The Distinction Between Authentication and Identification." 2000. URL: http://homepage.ntlworld.com/avanti/authenticate.htm (6/17/2003).

[13] "Biometrics: The Anatomy Lesson." Supply Chain Systems Magazine, November 2001. URL: http://www.findbiometrics.com/Pages/feature%20articles/anatomy.html (3/31/2003).

[14] Woods, Julie. "The New Opportunities for Biometrics." Business Solutions, March 2002. URL: http://www.findbiometrics.com/Pages/newopportunities.html (3/31/2003).

[15] Madigan, Michelle. "Proponents Push for Biometric IDs." Medill News Services. 30 October, 2002. URL: http://www.pcworld.com/news/article/0,aid,106533,00.asp (6/16/2003).

[16] Sullivan, Brian. "Biometric driver's license within five years?" CNN. 3 May 2002. URL: http://www.cnn.com/2002/TECH/industry/05/03/biometric.licenses.idg/index.html (5/30/2003).

[17] "What Are Biometrics' Basic Components and Processes?" International Biometric Group. 2003, URL: http://www.ibgweb.com/reports/public/reports/components_processes.html (8/14/2003).

[18] "Biometrics Standards." International Biometric Group. 2003. URL: http://www.biometricgroup.com/reports/public/biometrics_standards.html (8/14/2003).

[19] Miller, Allison. "Risks in Biometric-based Authentication Schemes." GIAC Level One Certification. 29 March 2000. URL: http://www.giac.org/practical/Allison_Miller_GSEC.htm (5/27/2003).