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

Biometrics: Hack Proof?

Bradley Beals

GIAC Security Essentials Certification (GSEC)

Practical Version 1.4

September 4, 2002

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

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

SUMMARY

Information Security has the difficult task of balancing the security of an organization with the convenience of the users. The more secure something is, the less convenient. Passwords are the de facto standard for authentication security, but since most users don't like the inconvenience of a secure (and difficult to remember) password, most users have passwords that are poor, or fair at best. Biometric devices are being touted as the solution for this weak link in the castle wall of security. But just like any technology that begins to merge into the mainstream of use, flaws begin to surface as their use increases.

This paper examines several security flaws that have been discovered in a number of biometric security devices. They range from simple to complex hacks, but they all reveal flaws in the fundamental technology. As biometric devices grow in popularity, it is important to become aware of the existing and potential flaws before jumping blindly onto this technology bandwagon.

INTRODUCTION

Our hero, Security Sam, must get to the heart of his enemy's lair, Hacker Headquarters. His pursuers are only minutes behind. He enters the lobby of the building and frantically searches for the correct entrance. There it is, in the back and to the right. He sprints, and arrives at the door out of breath. The door is locked, and requires fingerprint verification for access. What is our hero to do? Fortunately, Security Sam has come prepared. He pulls the severed finger of his enemy out of his pocket and places it on the scanner for verification. Access granted. He's in.



Fig. 1. Example of using severed finger on biometric scanner, from movie "The 6th Day"

What does it take to hack through a security perimeter with biometrics in place? Movies like "The 6th Day" show us that all we need is someone's severed finger. Or movies like "Minority Report" that want us to think all we need to gain access through a retinal scanner is the extracted eyeball from the authorized user. Using a severed finger or detached eyeball to hack biometrics may be an extreme example, but are biometric devices "hack-proof"?

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

BENEFITS OF BIOMETRICS

Biometrics is defined as "The automated use of physiological or behavioral characteristics to determine or verify identity."[1] This is essentially what passwords are doing: verifying the identity of the user. However, passwords in general are a weak security defense. As a broad rule, users select bad passwords ("dictionary" words without numbers or special characters), with the most cited reason being that they need to be easy to remember.

Passwords, which are still the standard form of authentication, have the advantage of being included in the software used, thus negating the need to purchase additional peripheral hardware. However, the disadvantages of passwords are many. ID's and passwords travel over the network and are susceptible to eavesdropping. They can be stolen or observed, and they are subject to replay attacks. Passwords can easily be shared with others, and given the proper access and tools, any password can be hacked with enough time. Although passwords have been the standard, we need something more secure. Biometrics claim to be the answer to that problem.

Biometrics can be anything that validates a user such as fingerprint scanners, hand scanners, face recognition, voice recognition, iris scanners, retinal scanners, and signature recognition. They are becoming more common and easy to use. For instance, some computer mice have the thumb scanner built right in to the side of the mouse, so additional hardware is not needed and your thumb is automatically scanned as you take hold of the mouse to start working.

Biometrics offers many benefits. For employers, it offers reduced costs (less password maintenance for support staff) and increased security. The increase in security is achieved because passwords aren't shared or compromised, and there is no badge sharing. Users benefit from biometrics since they no longer have to remember a password nor do they have to reset it on a regular basis. There is also the fact that they have a faster login time. Employees are also less likely to "forget" their finger or eye at home, unlike a badge. Retailers will see advantages like reduced costs, since it becomes much more difficult for biometric users to commit fraud. There is also the competitive advantage for businesses to be the first to offer biometrically secured transactions over their competitors. Consumers benefit from the added security since identity theft and fraud are exponentially more difficult for criminals to commit.

HACK-PROOF?

Biometrics offers many benefits, both to the work environment and to the marketplace. It is gaining momentum and popularity in many areas, and due to this, the prices for such devices are dropping. However, just as with any

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

hardware or software development, many holes are found once the product hits the market and is truly put through its paces.

Biometric manufacturers do their best to test their product as thoroughly as possible, but there are so many different factors to consider that the task can be daunting. One article noted that testing can produce different results depending on the group of people being tested. They tested a hand geometry system at Sandia Labs with a small error rate of 0.2%. When they ran the same tests at nearby Kirkland Airforce Base, they had error rates of 20%. What accounts for the vast differences in the tests? According to Dr. Jim Wayman, who conducted the tests, "The performance results were taken of one group of people in one environment, and not the performance of technology as a whole."[2] He also said that "…the errors were linked to the fact that unlike the Sandia test subjects, the Kirkland users were untrained, used the devices outdoors, and were not rewarded for correct usage."[3]

In the same way that the information security industry has been faced with trying to balance security and convenience, the manufacturers of biometric devices have to establish fault tolerance limits. The manufacturers use hardware and software to determine their limits. If the fault tolerance limit is set to a very narrow level, the security of the system is increased, but the user-friendliness of the system is likely to decline to a proportionate level since it is likely to come up with many false reads. If the manufacturer decides to increase the fault tolerance limit to allow for deviations that are likely to occur, this will make the system easier to use, but will, at the same time, decrease the level of protection provided by the biometric device.

In this discussion of the security of biometrics, three areas of vulnerability will be introduced. The first method attempts to fool the biometric device itself. This procedure makes use of the regular sensor technology of the system and does not try to bypass it. This would include artificial fingers for finger scanners, special contacts or fake eyes for iris or retinal scanners, and pictures for facial scanners. Using any sort of device to get the sensor technology to grant authorization would fall in this category.

The second approach also tries to fool the biometric system, but does so by bypassing the biometric input device and playing back to the system the proper reference data that was collected with some sort of sniffer device or software, commonly called a replay attack. An example would be a program listening in on the USB port. Later, the hacker can replay this recorded information to gain access.

The third scenario consists of attacks that try to compromise the database directly. This is more difficult to accomplish since it requires the hacker to be in

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

possession of database administrator rights and have permission to exchange sets of data that store the reference set used in the recognition process.

FINGERPRINT SCANNERS

One form of fingerprint scanner is the capacitive scanner, which measures the capacitance between the skin and scanner. As the distance varies, so does the capacitance. The scanner has 65,000 pixels, and when a finger is placed on the device, the finger acts as a capacitive pole. Of the fingerprint scanners researched, this appeared to be the easiest to hack.

In tests, the capacitive scanner was reactivated simply by breathing on the scanner's surface and the oil left by the latent fingerprint, which was then successfully authenticated through the biometric system. They just cupped their hands around the scanner, and slowly and gently breathed on it. On the screen you could slowly see the contours of the fingerprint reemerge. This is an amazingly easy and low-tech method for fooling a biometric device.

The testers were additionally able to fool the scanner by dusting the latent oily fingerprint with commercially available graphite powder (Ravenol). Then they placed some adhesive film on the scanner surface and applied pressure. Although the breathing method was only intermittently successful, when the latent fingerprints were high quality, they had an almost one hundred percent success rate with the graphite powder method.

Another test involved dusting drinking glasses and CDs for fingerprints with a professional fingerprinting kit. They would dust the fingerprints with the graphite powder, pull the fingerprint with adhesive film, place them on the scanner and apply some slight pressure. Their success rate was high with this method also.

Another type of scanner, the first and the most widely used technique, is the optical one. You place your finger above a prism or a diffracting grid and it is illuminated by light from LED's and captured by a small camera which measures the differences in the reflection. The tests that proved successful on the capacitive scanner were not able to fool the optical ones. For success, the testers had to move to using an artificial finger.

Tsutomu Matsumoto received much attention for his success in fooling the optical fingerprint scanners with "gummy" fingers. He made an artificial finger by using a live finger to make a mold, and he also made a mold by capturing a residual fingerprint. The material used for the artificial fingers was gelatinous material, similar to that used to make gummy worms or gummy bears, thereby incurring the name "gummy finger."

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

The first method Mr. Matsumoto used was to make a mold from a live finger. For the mold, he used a material called free molding plastic which is used for plastic models. (figure 2) Silicone rubber can also be used as an alternative. For the finger itself, he used solid gelatin sheets, which are used as ingredients for candies, molded desserts and jellied meats. (figure 3) As a substitute, gelatin powder can be used, however, it is more difficult to work with.



Fig. 2. Freeplastic used for fingerprint mold



Fig. 3. Gelatin sheet used for gummy finger

He put the free molding plastic in hot water. When it was soft, he removed it, let it cool slightly, and then shaped it into a small ball. He pressed a finger into the soft ball of plastic, removed the finger, and let the plastic harden, which took about ten minutes. (figure 4) Once this was finished, he moved on to the next step of creating an artificial finger.



Fig. 4. Series of pictures demonstrating creation of fingerprint mold

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

Mr. Matsumoto's next step was to dissolve the sheet of gelatin in boiling water. He sealed the mixing jar and waited for the gelatin to solidify as it cooled. Next, he reheated it in the microwave and then waited for it to cool again. Repeating this procedure several times reduced the number of bubbles in the mixture. The mixture was poured into the mold and then placed in the refrigerator to cool. In about ten minutes he had a gummy finger. The artificial finger was then carefully removed from the mold. (figure 5)

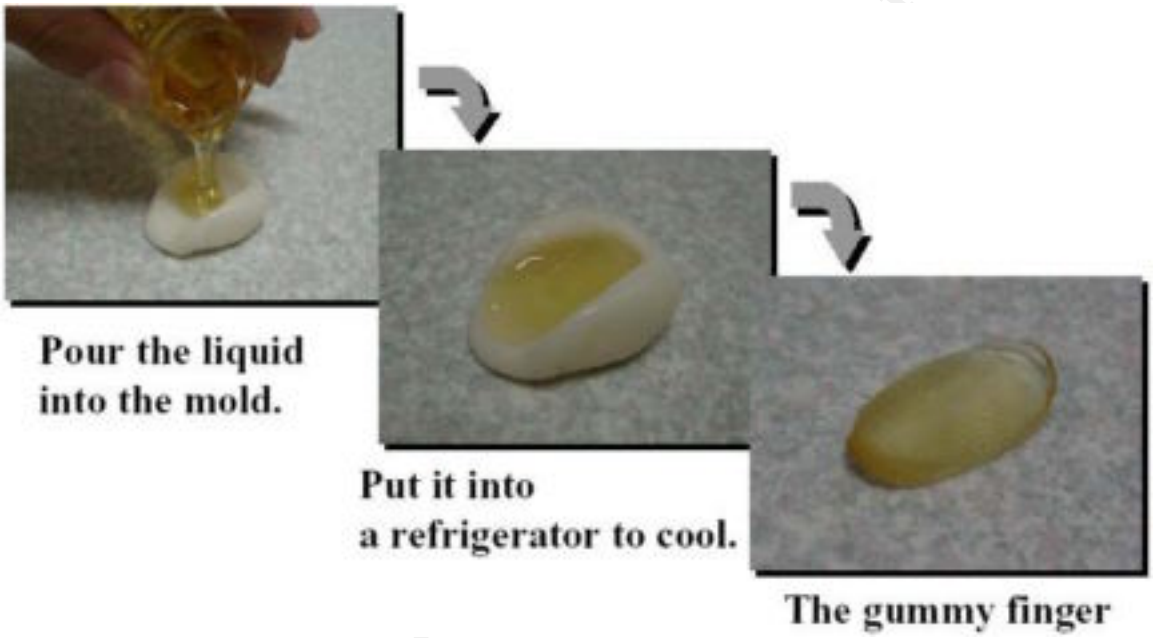


Fig. 5. Series of pictures demonstrating creation of gummy finger

Mr. Matsumoto was able to fool the biometric fingerprint scanners about 80% of the time with the gummy finger. However, an obvious obstacle to the success of this method is that you need to have the original finger in order to make the mold for the gummy fingerprint. Only the most naïve user would be fooled into giving out his/her fingerprint in this manner. This test only proved that the fingerprint scanners could be fooled with a gummy substance. But what if there was a way to create a mold from a latent fingerprint, like off of a coffee mug or glass? This is precisely what Mr. Matsumoto was able do. This process isn't as easy or cost effective as the previous example, but it works nevertheless. The process is diagramed in figure 6.

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

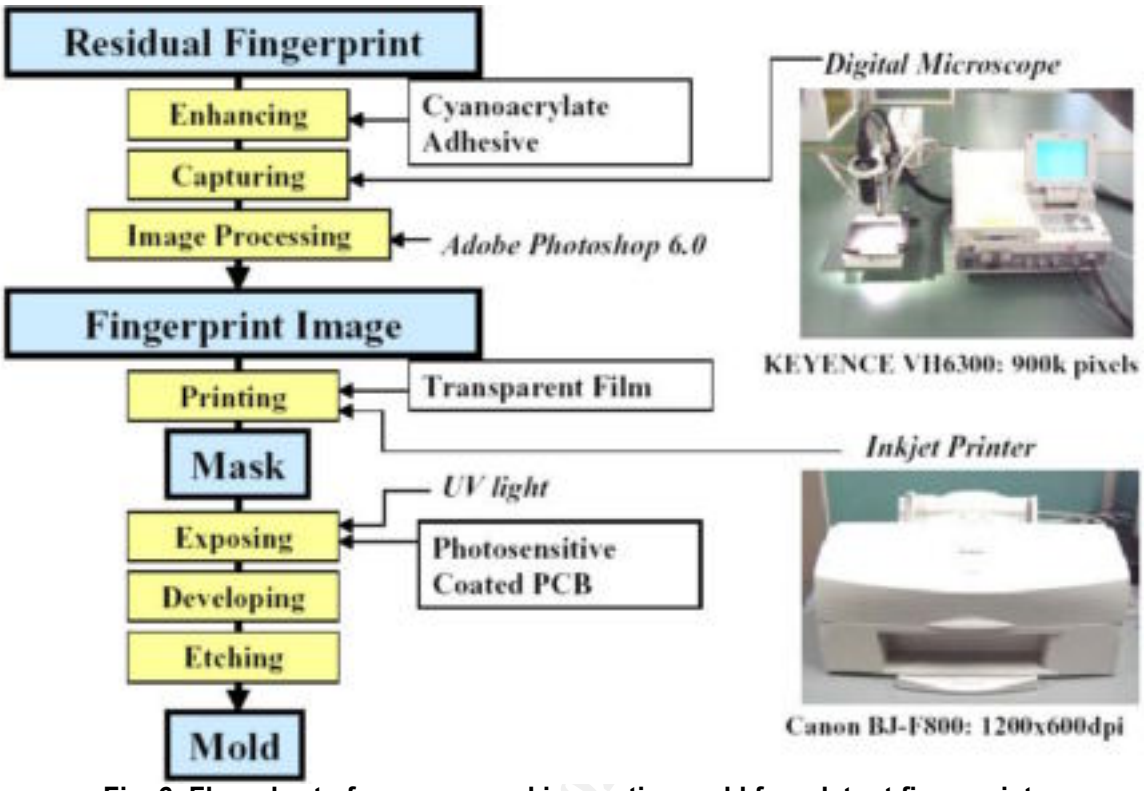


Fig. 6. Flow chart of process used in creating mold from latent fingerprint

The rather obvious first step in creating a latent fingerprint mold is to obtain a drinking glass with the desired fingerprint on it. Mr. Matsumoto enhanced the latent fingerprint with a cyanocrylate adhesive. After a short wait, the image was clearly visible. He took a picture of the image with a digital microscopic camera and using a photo enhancing software program like Adobe Photoshop, transposed the image (to get a mirrored image), then increased the contrast of the fingerprint. The fingerprint image was printed onto a transparency sheet with an inkjet printer. This was used as the mask.

To make the actual mold, a photosensitive-coated printed circuit board (PCB) was used and the newly created mask was attached to it. The PCB was exposed to ultraviolet (UV) light for at least 6 minutes, copying the image of the mask to the PCB. (He does warn that the UV rays are harmful to the eyes and should not be looked at.) He developed the PCB which removed the unneeded photosensitive material and exposed the copper. The final step in making the mold was to etch the developed PCB which removed the exposed copper, leaving a mold of the fingerprint. At this point, the same process was followed as before in creating the gelatin liquid and pouring it into the newly formed mold. (see figure 7)

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

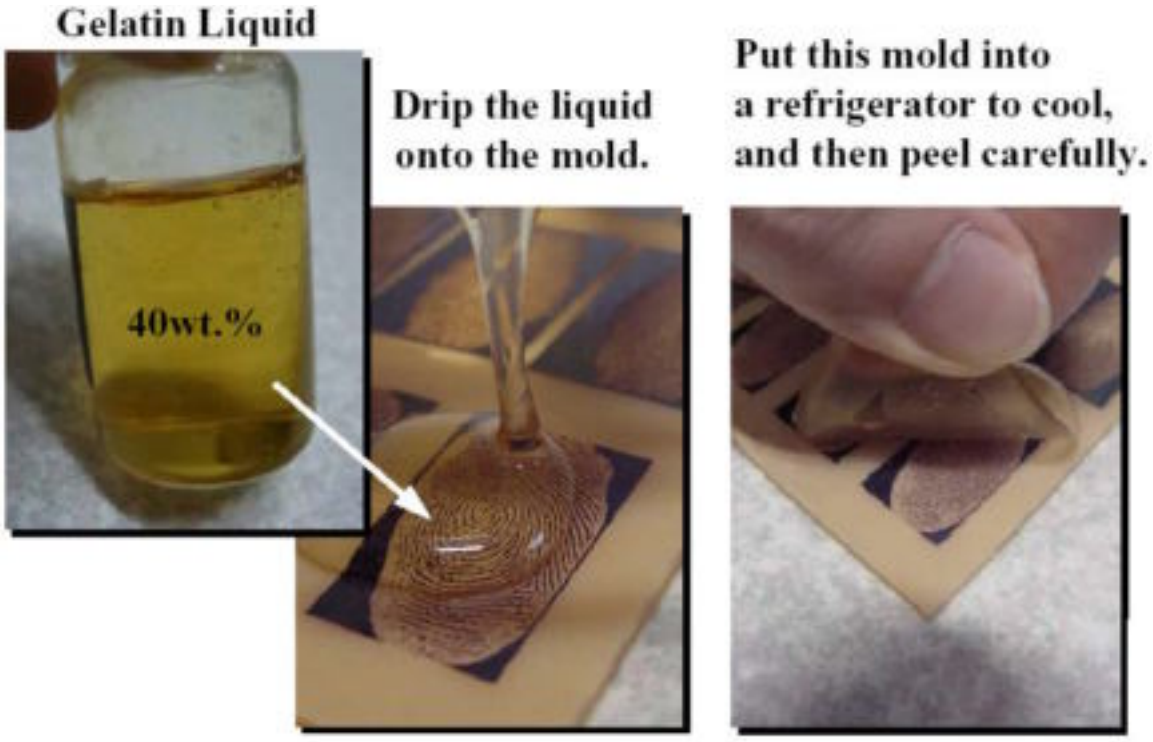


Fig. 7. Series of pictures demonstrating creation of gummy finger from latent fingerprint mold

In his testing, Mr. Matsumoto tested eleven different fingerprint biometric devices, all commercially available. He was able to reliably fool all of them. These devices included both optical and capacitive scanners, and some even had live finger detection features. In some cases the gummy fingers had to be moistened, and although it took some practice to get it right, he was still able to get them to work. One of the advantages of the gummy fingerprints is the ability to attach the thin fake print over your own fingerprint, and in the case where guards are watching, appear to use your own finger. Once through the checkpoint, you can eat the evidence!

In another test of biometric security, an Australian National University student was able to hack through the device using the information stored within the system itself. Chris Hill worked on discovering the way the system stored the template information and then created images that had enough similar "features" of the desired fingerprint to trick the device. He said, "Really all I had to do was crack the code of the template, so the images I created that were accepted by the security system did not even look like thumbprints they just displayed the characteristics required by the computer program."[4]

Since many biometric devices use the Universal Serial Bus (USB) port, it is important to note that security is not one of the USB's fortes. Since it allows users to swap, add and remove devices while the system is running, it gives potential hackers an advantage. The hacker could exchange biometric scanners

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

for their own device and play back the data to the computer that was captured while eavesdropping on the valid user's login.

Another example of the USB security hole is a hardware analyzer like the USB Agent by Hitex. This device captures data from the USB cable directly and is virtually invisible. "A USB Agent latched on to the cable records all transmitted data, transferring these to a foreign PC. An assailant can then, with the aid of the software that goes with the device, analyze on the foreign PC the protocols used by the target PC and filter out the relevant data packages."[5] Exporting the data to a text file then makes it possible to get enough information to recreate a successful login.

Taking a slight detour to face-recognition systems, a study has been done to show that these systems are much better at matching smiling faces than those with dead-pan expressions. As identification databases become larger, it will become increasingly difficult for computers to find a match. Researchers have found that smiles, even between people who look very similar, reveal different features and uncover more details of their underlying muscle and bone structure. Interestingly they also found that angry, frowning faces are even more distinguishing than smiling ones. So the less expression a criminal shows, the harder it is for the software to find a viable match.

IS BIOMETRICS A VIABLE SOLUTION?

Biometrics has been touted as the answer to our security authentication problems. However, I've shown hole after hole in this security "solution". This doesn't mean biometrics should be tossed out like day-old doughnuts. "Just as a firewall does not constitute a network security solution but rather a component of a defensive strategy, biometrics could be viewed in the same manner."[6] Today, auto thieves don't try to get your car key and make a duplicate, they just try to by-pass the alarm and ignition system to get the car started. In the same way, biometrics can't be viewed as a cure-all for authentication security problems. We need to have security defense in depth.

Other issues needing discussion are: What happens when the part of the body getting validated is somehow damaged, such as a finger getting badly burned or deeply cut? Or, if someone does manage to create a fake fingerprint from your finger, how is that issue resolved, since a finger can't be easily changed like a password can?

Although there are many aspects of biometrics that are being fine-tuned and still need to be addressed, biometrics can and should be integrated into every company's "defense in depth" security policy. There are several ways that biometrics can be used that greatly increase security instead of weakening it.

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

The International Biometric Group lists four different policies that allow biometrics to play a key role in exponentially increasing authentication security.

- **Randomization of verification data**. If users are asked to enroll more than one biometric sample - for example, three fingerprints or two distinct voice patterns - the system may randomize the biometric data it requests for verification, thereby slightly reducing the likelihood of spoofed data being usable for verification. Such a system may also require two fingerprints for verification, such that an imposter would have to locate two "target" fingerprints with which to defeat the system.

- **Retention of identifiable data**. In most transactional biometric systems, identifiable data is destroyed immediately after template generation. Retaining image data, though posing substantial privacy and storage challenges, may provide a means of resolving spoof claims. In many cases spoofed biometric data will be evident upon inspection of the actual sample (inspecting the template, of course, would be useless). Retention of this data strengthens a system's audit trail, and forces imposters to create data that looks like a biometric sample to the naked eye as well as to an extraction algorithm.

- **Using multiple biometrics**. Multiple biometric authentication is often proposed as a means of solving the liveness problem, as it is clearly much more difficult to spoof two biometrics in tandem or in sequence than to spoof one. However, implementing multiple biometrics is currently much more difficult than it seems. Process flows for verification are generally not compatible with the provision of more than one biometric characteristic, due to environmental, cost, or equipment limitations. In certain environments, multiple biometric implementations can be deployed effectively; however, it is not the cure-all that it would seem to be at first glance.

- **Using multi-factor authentication**. Ultimately, the use of multi-factor authentication - using biometrics with smart cards, tokens, even passwords - reduces the convenience provided by biometric systems but reduces the likelihood of biometric systems being spoofed. An imposter would need both the token and/or the secret along with imposter data in order to defeat the system. In certain biometric systems - identification systems, for example - this is not viable.[7]

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

CONCLUSION

Biometrics offers a considerably increased level of security to authentication methods. In addition, biometrics has the advantage of not being forgotten or left at home, and saves companies money in support costs. However, there are still many security holes that need to be addressed. Just as a firewall is not a silver-bullet, single-solution to network security, neither should biometric devices be touted as the end-all to authentication security problems.

Biometric devices have flaws, but so does every other security hardware and software solution. Biometric security measures offer such a strong level of security, that they cannot be thrown out or ignored simply because a few flaws have been discovered. They need to be incorporated into an organization's already strong defense in depth. Biometrics, especially in conjunction with passwords or passcards, offers the level of security that we need at this stage in the development of information security.

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

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

ENDNOTES

[1] *How is 'Biometrics' Defined?* International Biometric Group. <http://www.ibgweb.com/reports/public/reports/biometric_definition.html> (August 14, 2002).
[2] Harrison, Ann. "Researcher: Biometrics Unproven, Hard to Test." August 7, 2002. <http://online.securityfocus.com/news/566> (August 15, 2002).
[3] ibid.
[4] Jackson, Catriona. "Security System Gets Thumbs Down From Honours Student". *The Canberra Times* June 13, 2002. <http://canberra.yourguide.com.au/detail.asp?class=News&story_id=155922&subclass=local&m=6&y=2002> (July 11, 2002).
[5] Thalheim, Lisa, Jan Krissler, Peter-Michael Ziegler. "Biometric Access Protection Devices and their Progrmas Put to the Test". May 22, 2002. <http://www.heise.de/ct/english/02/11/114/> (July 11, 2002).
[6] Penny, Wayne. "Biometrics: A Double Edge Sword – Security and Privacy" SANS Institute. March 18, 2002. <http://rr.sans.org/authentic/sword.php> (June 17, 2002).
[7] "Liveness Detection in Biometric Systems". International Biometric Group. <http://www.ibgweb.com/reports/public/reports/liveness.html> (August 14, 2002).

REFERENCES

Chun, Marilyn. "Authentication Mechanisms – Which is Best?" April 5, 2001. <http://rr.sans.org/authentic/mechanisms.php> (June 17, 2002).

"Fingerprint Recognition Technology." On World. <http://www.onworld.com/html/biometrics.htm> (August 23, 2002).

Harrison, Ann. "Researcher: Biometrics Unproven, Hard to Test." August 7, 2002. <http://online.securityfocus.com/news/566> (August 15, 2002).

"How is 'Biometrics' Defined?" International Biometric Group. <http://www.ibgweb.com/reports/public/reports/biometric_definition.html> (August 14, 2002).

Jackson, Catriona. "Security System Gets Thumbs Down From Honours Student". *The Canberra Times* June 13, 2002. <http://canberra.yourguide.com.au/detail.asp?class=News&story_id=155922&subclass=local&m=6&y=2002> (July 11, 2002).

"Liveness Detection in Biometric Systems". International Biometric Group. <http://www.ibgweb.com/reports/public/reports/liveness.html> (August 14, 2002).

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. "Impact of Artificial "Gummy" Fingers on Fingerprint Systems". January 24, 2002. <http://cryptome.org/gummy.htm> (July 11, 2002).

Matsumoto, Tsutomu. "Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies – A Case Study for User Identification". May 14, 2002. <http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.html> (July 24, 2002).

Penny, Wayne. "Biometrics: A Double Edge Sword – Security and Privacy". SANS Institute. March 18, 2002. <http://rr.sans.org/authentic/sword.php> (June 17, 2002).

"Software 'Has More Chance of Catching Smiling Robbers'". May 30, 2002. <http://www.smh.com.au/articles/2002/05/30/1022569804486.html> (July 11, 2002).

Thalheim, Lisa, Jan Krissler, Peter-Michael Ziegler. "Biometric Access Protection Devices and their Progrmas Put to the Test". May 22, 2002. <http://www.heise.de/ct/english/02/11/114/> (July 11, 2002).

Van der Putte, Ton, Jeroen Keuning. "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned". Atos Origin. September 21, 2000.

"What are the Benefits of Biometric Technology?" International Biometric Group. <http://www.ibgweb.com/reports/public/reports/biometric_benefits.html> (August 14, 2002).

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

FIGURES

Fig. 1 *The Sixth Day.* Directed by Roger Spottiswoode. Produced by David Coatsworth, Jon Davison, David Latham (III), Mike Medavoy, Daniel Petrie Jr., Arnold Schwarzenegger, Cormac Wibberley, and Marianne Wibberley. Written by Cormac Wibberley and Marianne Wibberley. DVD. Columbia Pictures, 2000.
Fig. 2 Matsumoto, Tsutomu. "Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies – A Case Study for User Identification". May 14, 2002. <http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.html> (July 24, 2002).
Fig. 3 ibid.
Fig. 4 ibid.
Fig. 5 ibid.
Fig. 6 ibid.
Fig. 7 ibid.

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

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