Joseph A. Pippin, Jr. An Examination of the Risks Associated with Widespread Deployment of Current Biometric Technologies for Data Security. A Master's Paper for the M.S. in I.S. degree. January, 2005. 39 pages. Advisor: Jeannie Walsh

Biometric technologies have been under development for years. Finger, face, and iris scanners are already in place in both high and low security environments. Over the next decade, many companies are preparing to deploy biometric scanners in everything from cars and pocketbooks to corporate offices and ATMs. The proliferation of a technology that is currently unregulated, non-standardized, and uses questionably secured databases to hold unique, non-secret, and irreplaceable personal identifiers - whether fingerprint, iris, facial scan, or some other - is a risky proposition. This paper looks at the myriad complications and caveats of biometric technology, and should serve to caution anyone, especially decision makers and influencers who manage data access and those who may consider implementing or authorizing the use of biometrics in their data environment.

Headings:

Biometrics

Biometrics -- Risks

Information Security -- Biometrics

Computer Security -- Internet -- Security Measures

Computer Security -- Biometrics

Information Policy -- Records Management

AN EXAMINATION OF THE RISKS ASSOCIATED WITH WIDESPREAD DEPLOYMENT OF CURRENT BIOMETRIC TECHNOLOGIES FOR DATA SECURITY

by
Joseph A. Pippin, Jr.

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

January 2005

Approved by

____

Jeannie Walsh

Table of Contents

INTRODUCTION

Advancing technological innovations are using human biological information to protect data and data access. Devices built to authenticate or identify an individual based upon biological markers are part of a field of science known as biometrics. A person’s fingerprint whorls and swirls, their hand and face geometry, their iris and retinal patterns, their voice pattern, and even the composition of their sweat are all examples of biometrics. In our daily lives, the act of recognizing another individual requires us to interpret biometric information. Although the term “biometrics” may lack widespread recognition in homes across America, the field’s influence is certain to become nothing short of ubiquitous in the coming years. Biometrics of the past and present – even those as commonplace as the hand-written signature – are already being enhanced or outright replaced by advancing biometric techniques. Yet many of the elements in biometric research are relatively unknown to the Information Science community. Still the province of Computer and Mathematical Sciences, it is necessary for IS to become more acquainted. How appropriately these biometric advancements are applied to securing data, their practicality in everyday application, their effectiveness and accuracy, and how heavily we rely upon them to protect data are timely issues. There is a great need for more study and research before we allow these newer, more personal, and potentially invasive biometric technologies to enter our lives, because these technologies carry the possibility of becoming so heavily ingrained and accepted in our daily routines that we may find ourselves unable to distance ourselves from them.

Biometrics could open the proverbial Pandora's Box. Despite what the sales and marketing forces of the manufacturers might have us believe about the security of biometric technologies, they are far from perfected. If your fingerprint, your facial image, or your retinal pattern are permanently duplicated or even just electronically hijacked for a short time, your life could change irrevocably. The possibilities for illicit use of a stolen biometric are disturbing, and as companies implement biometric devices with the aims of better security for information access, those who manage the equipment must be aware of the risks that accompany such implementations. Furthermore, companies must address biometric privacy concerns rather than assume tacit consent from employees and customers who may not be cognizant of potential risks. Such measures are necessary because these proprietary systems appear to be significantly vulnerable to attack.

Researchers who intentionally attack and break biometric devices are finding that many of them lack sufficient reliability and security against circumvention or theft. Unfortunately, much of society seems oblivious to the dangers of freely giving their fingerprint or any other biometric. In May 2002, Indivos Corp. put fingerprint scanners in a Thriftway in West Seattle, Washington. A reporter from the Seattle Post-Intelligencer, an online newspaper, wrote that the customers "had few concerns about handing over their index fingerprint and credit card number to Indivos [1]." The reporter quoted a regular customer as saying "I figure they must have perfected it or they wouldn't be doing it [1]." The naiveté of this comment, and the likelihood that such beliefs are far too common, is cause for concern. In the same news report, Indivos claimed that it would not "sell, rent, license, or share personal data [1]." How can the general public trust that this policy will remain in force for a lifetime? Indivos is likely to have those customers on file for many years.

The issue of biometric ownership is fraught with difficult issues. In the Post-Intellegencer story, the reporter mentioned that Indivos was suing another grocer's biometric payment processing company, Biometric Access Corporation, for copyright infringement. Hypothetically, although Indivos lost the case, Biometric Access Corporation could have countersued and won rights to Indivos' databases. If Indivos were divested or merged with another company, that action could adversely affect the consumers' privacy and security. The privacy rights might not remain intact. There might not be an opt-out period offered before the data transfer. Since biometrics exist as a wholly unregulated industry, lacking a coherent set of standards and authoritative bodies to provide oversight, the Thriftway example raises many privacy issues that deserve investigation. If you have a grocer's savings card, you can opt not to use it if you desire and you may regain some small amount of anonymity. But once your fingerprint is in use by your grocer and in other various stores and settings, across multiple vendors and applications, database sharing becomes no small matter. History and logic tell us that profit, not privacy, is likely to be more important to the corporations in control of this data.

This study examines the current state of the art in biometric technology research and examines its limitations and threats to its security. Biometric devices must contain safeguards to prevent the mining of personal data by untrusted sources. Any biometric device that scans accurately but holds the potential to disclose personal information about any or all subjects through known circumvention techniques, especially without a full disclaimer of such possibilities to said subjects, should immediately raise questions about privacy and security.

BACKGROUND

Banking and financial systems are arguably some of our nation’s most secure systems. Yet, in February 2003, more than 8 million card numbers were stolen from Data Processors International, a processor for Visa, MasterCard and American Express [2]. If a bank’s, their subsidiary’s or processor’s credit card database servers are illegally accessed and card numbers are stolen, the issuing bank can void the numbers, stop transaction acceptance on those cards, and notify customers that a replacement card is forthcoming. Consider a server full of biometric data. If credit card numbers can be stolen, and presumably decrypted, from secured financial institutions, then biometric data is no safer. If social security number fraud is difficult to fix once the number is in circulation illegally, then an individual will have difficulty convincing the bank that it “wasn’t my retinal image” used to withdraw funds or to make a purchase [3]. An important theme in this discussion is that the same biological markers that make us unique are also irreplaceable; biometrics cannot be “reissued.”

Proponents of biometrics argue that the traditional method of security – passwords – are easily forgotten or hacked [4]. There is no reason to believe that a biometric database would be any less prone to hack or attack than any other computer system, specifically due to the fact that encryption technology is the same regardless of what object is encrypted [5]. As biometrics gain widespread acceptance, a person’s unique biometric information may be stored in multiple databases in multiple locations.

Credit card number databases, even at the corporate level, are carefully monitored and secured to guard against theft of the information. But consider this situation from an August, 2004 Associated Press news release:

> “BJ's Wholesale Club Inc. attracts shoppers to its stores by putting thousands of discounted products under one roof. It wasn't hard to attract cyberthieves either, with databases that amass credit card numbers in huge numbers. The theft earlier this year of thousands of credit card records from the nation's third-largest warehouse club illustrates the potential for massive-scale identity theft whenever so much purchase-enabling information is stored in one place. It also illustrates how difficult the cleanup can be...” “..Philadelphia-based Sovereign Bank covered about 700 fraudulent transactions from the BJ's theft and had to reissue 81,000 cards twice, at a cost of about $1 million... [6]”

Replace the word “credit card” or “card” with the word “biometric” in the above situation. Since biometrics cannot be reissued, 81,000 biometrics would be permanently compromised. We assume that credit card databases are encrypted and secured with the latest technology by companies with years of financial protection experience, and yet the example above shows otherwise. It is not likely that biometrics databases share the level of robustness held by our society’s best databases, and since our best are occasionally and provably violated, it is only logical to acknowledge that we can expect similar results with biometric ones. When a single, poorly managed biometric database is breached, it is difficult to imagine to whom will we turn for help. Financial institutions may be able to offer advice for vendors that show concern about liability. The government may regulate the industry after a given number of failures create public outrage. However, the unregulated biometric vendors would be forced into handling the situation quickly and appropriately only by self interest and perhaps goodwill, because unlike federally insured banks, they do not have federal regulations about the way information is handled. Setting standards and creating oversight mechanisms may help address such dangers.

One relatively weak and often used biometric already suffers from theft – a person’s signature. Signatures are often forged, and as a result, our society has learned not to put much trust in the signature by itself. Our institutions have developed safeguards, such as notaries and guaranty stamps, to attest that a person actually signed in cases where a signature is most important. But the popular press and many manufacturers are putting too much faith in biometric technologies – this relatively young technology repeatedly receives accolades of how it is the answer to passwords and that it will protect our data in the future. In July 2004, CNN.com's Technology site presented a report entitled "Biometrics to keep handbags safe [7]." In November 2003, USA Today asked, "Will that be cash, fingerprint, or cellphone [8]?" Recent automobile television ads show luxury cars that open and start with the press of a finger.

Biometric technology has the potential to make significant changes in the way we make data transfers. Consequently, the Information Science community must be prepared to help develop the biometric equivalents of bank security to guard our irreplaceable personal biometric data. If the field of Information Science is to prepare those who may control and provide access to these databases, we should investigate the available research, gathering a clear notion of how well the technology works so that we may logically debate the issues and create solutions to mitigate the risks before and after these devices are implemented.

PROBLEM STATEMENT

The biometric technologies available today are often used for the securing of data and information access – either physical, electronic, or both. Within each type of biometric – facial, finger, palm or ear geometry scanning; iris or retinal imagery scanning; sweat composition measurements; blood DNA matching; etc. – many options are available to the consumer, and each biometric type varies in its ability to provide accurate results. These recognition inaccuracies are known in biometrics as "false positives" and "false negatives," both of which will be explained in a later section. Regardless, all biometric technologies tend to focus on one of three applications – authentication prior to access, authorization for access rights, or 1:1 identification of an individual [9]. The appropriate usage of an application in a given circumstance is a subject of much debate in the biometric field because biometrics do not perform as well in identification as they do in authentication [9]. Furthermore, biometric applications collect and store unique personal data without proof that the biometric data storage methods are secure against proven attacks [10].

The intent of this research is to collect and organize academic and field investigations of the biometric technologies available for use in data security applications, drawing upon previously published risk assessment studies and published field discussions. There are many experienced researchers who have tested existing biometric methods and applications, and these researchers have found the technology in varying states of adequacy for data security [5,10,12,15,18,20,26,27]. Thus, the goal is to provide an assessment of the risks and liabilities of these biometric applications in order to add to the growing body of knowledge that recognizes both the potential rewards and the caveats of using personal biometric data for identification and authentication.

The inherent and potentially unavoidable risks of biometric technologies need to be presented to and acknowledged by both academia and the popular press before such technologies inevitably gain greater acceptance – possibly to the point of societal dependence. As such, the question arises as to whether or not there is enough user data protection to justify the risks of biometric implementations, and whether or not the risks of theft of biometric data are worth the reward of increased data security and more reliable user authentication. While this discussion does not presume nor intend to make a decision for society at large, it will hopefully elucidate whether or not the current technology is ready for the challenges of reliable biometric implementation.

ANALYSIS

BIOMETRIC ATTACK METHODS

Falsification Attacks

“The main advantage of capacitive sensors is that they require a real fingerprint.”

-Bergdata Biometrics GmbH, biometrics manufacturer.[11]

The optical sensors used in some biometric devices, including many fingerprint and palm scanners, often accept forged biometrics because they look only at the physical details, such as fingerprint ridges. This is because optical sensors view the input as a static set of information. One analogy is to think of such a scan as a photograph that is mathematically analyzed by the equipment once it is captured. Another popular type of sensor – capacitive – measures the electrical resistance of a material and is expected to confirm “liveness” in a biometric. Research has shown that these types of testing devices are susceptible to both conductive silicone rubber fingers and gelatin mold fingers. Gelatin mold fingers are very easy to make. Soft molding plastic is used to take a fingerprint impression, and gelatin, which is dissolved in hot water and then cooled, is poured into the mold. The result is a highly realistic “gummy” finger [10]. In tests of eleven different commercially available readers, including models by Secugen, Ethentica, Sony, Siemens AG, NEC, OMRON, and Compaq, Tsutomu Matsumoto's lab at Yokohama National University in Japan showed that it is a trivial exercise to fool both optical and capacitive sensors using a gummy or silicone finger [10]. His group succeeded in both the enrollment and the verification of the fake fingers against enrolled fake and enrolled live fingers. The success rate of the falsification attack averaged more than 80% against all of the devices [10].

During the process of enrollment, the invariant and discriminatory parts of the user's biometric are scanned and encoded as a template [14]. If the sensors do not detect an authentic finger, for example, they are purportedly designed to not enroll the biometric. Nevertheless, all eleven sensors were fooled repeatedly by Matsumoto's gummy and conductive silicone fingers. Not only did they enroll and verify against their own fake template, but also against a real finger's template [10]. Both breaches are condemning, but the threat against the real finger may be a bit more disturbing. If a fake finger matches only against its enrolled fake finger, then the criminally intent enrollee could only hope to successfully forge and enroll a finger for various malevolent, but potentially limited, purposes. Since this fake will not match a real and expected user of the system, it may or may not be given access rights, depending on the system and what the system is designed to protect. If, however, a fake can be created that matches against a real and existing entry, as Matsumoto has shown conclusively, then every user of the system becomes a potential target of theft.

Replay/Resubmission Attacks

Interception and reuse of another's biometric is known as a replay attack. The copied biometric is replayed, or resubmitted, as if the person were still present. Replay is similar to a falsification attack because the submission is a forgery, but it differs in that the biometric is strictly pre-existing on the system; it requires an enrolled subject. A replay attack uses various methods to resubmit the biometric in an attempt to gain access. For biometric devices that use capacitance as a security measure, one simple method that has been employed with moderate success is to blow humid air on the device. With this method, the fat deposits of the last latent image are reactivated and create just enough electrical current to fool the sensor [12].

After the German Federal Institute for Information Technology Security and the Fraunhofer Research Institute refused to publish the results of extensive security testing on several biometric device manufacturers, *c't*, a German computer trade periodical in publication for over twenty years, decided to test biometric devices and publish the results. A majority of devices readily available for biometric security are fingerprint scanners [12, 13]. Face and iris scanners battle for second and third in the market [12]. Since all other biometric types combined make up less of the market than these three, *c't* decide to test eleven total biometrics from the first three categories [12]. Among six capacitive fingerprint scanners from Biocentric Solutions, Cherry, Eutron, Siemens, and Veridicom, two optical fingerprint scanners from Cherry and Identix, and one thermal fingerprint scanner from IdentAlink, *c't* found many flaws [12].

After experiencing marginal success rates with the warm air blowing technique, *c't* researchers used bags of water to apply even pressure to the latent fingerprints on the device. This technique worked intermittently, but often enough to raise concerns:

> "The probable reason for this phenomenon [is] that the capacitors of the capacitive sensor are sensitive to humidity. Damp air that, for instance, condenses on the sensor's surface where there are residues of fat causes the relative dielectric constant on the sensor's surface to change thus leading to a change in capacitance which the device interprets as a release signal inducing it to undertake a measurement [12]."

One sensor showed particular susceptibility to the water-filled balloon method. Once the sensor was dusted with graphite powder, and after the visible fatty residue was covered with adhesive film, pressure was applied using the balloon to achieve a near 100 percent success rate [12].

Iris scanners and facial recognition scanners are also susceptible to attacks. In other tests, *c't* researchers took photographs of eyes enrolled in the system and used an inkjet printer to produce photographic quality printouts of them. Once the scanner's method of detecting liveness was determined – eye depth in this case – the researchers found a novel approach to circumvent the test. Unable to get the scanner to accept an image of an eye as real, they cut out and removed the pupil from the printout, then put their own eyes behind the image and thereby fooled the iris scanner [12]. Facial recognition scanners fell to *c't* researchers with hand held photographs and replayed AVI video clips that showed a few seconds of a head turning [12].

In fairness, *c't* mentions that the device manufacturers of their tested products state that the devices are not for use in high security environments. Several of the devices are merely mouse or keyboard sensors, which are likely sold as much for the novelty and public fascination as for security. Nevertheless, ubiquitous biometric devices will not all be used in high security environments, yet they should still be expected to perform appropriately if their job is to protect access. The novel application of such biometric scanners is disconcerting because it creates both a false sense of security and markets the low-end devices as somehow more useful than a password, despite the exposed flaws of the former. Because biometric devices are available with varying degrees of quality, individual consumers and companies may not be able to find out which ones to trust without ongoing, independent testing.

Man in the Middle/Channel Attacks

As with man in the middle (MITM) attacks on networks, if someone can eavesdrop on the conversation, they have effectively breached security. In biometrics, MITM attacks are sometimes referred to as channel attacks. If a device can be attached to a biometric scanner and listen to the channel during the enrollment phase, a biometric could not only be intercepted, but the device's response to enrollment may allow other clues towards penetration of the system. The pervasive use of scanners in public and private realms will make MITM attacks possible. Compounding the issue, interception of a biometric with a channel attack could create the opportunity for replay, falsification, and hill-climbing attacks on the devices.

Hill-Climbing Attacks

As previously stated, users are added to a biometric database through the process known as enrollment, at which point a template is created. When a user presents a biometric for verification, a value is calculated between the submitted features of the user and the user's stored template in a process known as matching [14]. The biometric program processes the data and returns that value as a score [14]. A skilled MITM attacker who is capable of gaining access to a user’s template and who is able to introduce a rogue application – one which captures the score and submits biometric data – can defeat the system using a hill-climbing attack [14, 15]. With a fingerprint system, for example, such an attack would be performed by a pairing and submitting a random fingerprint with the user’s template [14]. The attacker submits multiple samples and merges those that create a positive score, eventually fooling the device and gaining access [15]. The BioAPI Consortium [16] has recommended that the template scores be quantized, which means that small changes to the image will not affect the score enough to be useful in a hill-climbing attack. Nevertheless, Adler [15] was able to achieve a 95%CI with a hill-climbing attack against a system that used the consortium’s recommended quantization.

All of the attacks discussed so far have some similarities that may blur what distinguishes hill-climbing from them. Hill-climbing may be considered a variation of the MITM attack, but it is not a replay attack because the submission is uniquely created for each attempt at access. Since the submission requires an existing template, hill-climbing is also not a falsification attack as previously defined, but it could be argued that it is a subclass.

Decision Override Attacks

Decision override attacks are another class of attack. This type requires substantial access to a biometric device’s decision making processes. If the matcher application and the database do not reside in a secure location, the ability of an attacker to alter the final result, or decision, of the biometric device is a theoretical possibility [17]. This issue is open to further research.

Forced Action Attacks

Forced action attacks occur when a person is put under duress to elicit biometric presentation. For example, a criminal may force a person to use her biometric at gunpoint in order to gain illicit access. Another example would be that a user is drugged or rendered unconscious and the biometric is used thusly. These types of attacks are not against the system as much as the person, which makes them all the more dangerous as a possible threat [10].

If biometric devices come to protect a myriad of valuable goods, there will exist a greater incentive for criminals to harm people for access to those goods. If such devices allow us access to a bank's ATM at the scan of an eye or touch of a finger, then the same criminal that once had to locate a person with a bank card and force him to operate the machine no longer has to linger around an ATM just to find someone with a bank card to attack. The act of obtaining the "key" can now be planned miles away in any less secure environment. Thus, an affluent person in expensive clothing may bear additional risk when a criminal is looking for a hand or a head to force against a scanner.

OTHER BIOMETRIC ISSUES

False Positives and False Negatives, Acceptance and Accuracy, and Usability

Fault tolerance limits pose a weighty challenge to biometric technologies and are a confusing subject to both the layman and the well informed. Biometrics devices must not only validate the authentic submissions but also reject the equivocal ones. If the system fails to do one or the other, it is not useful as a security device. An issue that biometrics vendors must deal with is the need to tweak false rates of both rejection and acceptance. A false rejection is interchangeably referred to as a false negative; both meaning the rejection is wrong – there should have been an acceptance. In similar fashion, a false acceptance is also referred to as a false positive; meaning the acceptance is wrong – there should have been a rejection. The vendor wants to minimize both of these error rates as much as possible. Of critical importance is the ability to fail gracefully; it is better to falsely reject and inconvenience someone than to falsely accept them and risk a security breach.

Further complicating the issue is that the false rejection and false acceptance rates are subsets of the overall acceptance (or verification) rate – a rate which can be viewed in two different ways: the vendor's overall acceptance rate, which is determined by the vendor's adjustments to the hardware and software; and the "real world" or "actual" overall acceptance rate, which is based upon what happens mathematically when the system is actively challenged to authenticate and reject users. In order to understand overall acceptance rates, we must separately consider the physical limitations of the system against the mistakes of the hardware and software.

After a given number of subjects are put through a system, an overall acceptance rate is calculated as a percentage. If nine users are let in out of ten, then the “actual” overall acceptance rate is 90%. However, this is just the rate of authentication based upon how many users made it through the system. This “actual” overall acceptance rate is not useful for determining effectiveness of a system without another piece of information.

The important value to determine is *how many of the 90% accepted were valid user claims*; in other words, how many of those nine *should* have been let through. If the number of valid user claims against the system is not known, the effectiveness of the system is indeterminate. After all, if 100% of the claims were valid, then 90% is a poor statistic. If, however, 90% of the claims were valid and 10% were falsifications, the statistic is ideal; it is the golden mark that manufacturers and vendors have a great deal of difficulty hitting – and with good reason.

One reason the acceptance issue is obtuse is because in the example, the 90% “actual” overall acceptance rate is the best the hardware and software can do in a real world situation; the hardware and software combined can perform no better than 90% acceptance. As such, this 90% acceptance rate translates as the manufacturer’s 100% setting for the device. The situation of hardware and software limitations make the accuracy rate data confusing, which leaves an opening for vendors to state misleading facts without actually making false statements. For example, even though the aforementioned device cannot attain a 100% accuracy in the real world, it can perhaps attain 95% of the hardware’s 100% – which we know from our hypothetical testing is

90%. So if the vendor states that the device has a 95% accuracy rate, even though 95% of 90% is only 85.5%, the statement is disingenuous without being false. Therefore, how this number is derived is always crucial in judging a manufacturer’s claims, because a 95% accuracy rate for a device that can only attain an *actual* 60% is a device that has a effective accuracy rate of 57%. And since this derivation is from the maximum setting that the example device can achieve, scanning percentages can only go down when the vendor adjusts for too many false positives or false negatives.

A manufacturer will adjust the overall acceptance rate based upon how aggressively and appropriately they desire the false positives and false negatives to be handled by the software and hardware. Figure 1. shows the decision process of the biometric system. A manufacturer can ease the restrictions on what defines a match; fewer points of comparison, larger allowances for physical variations, greater tolerance for partial matches, broading the scoring calculation range used to determine acceptance, etc. Theoretically, even if a vendor were to set the system to accept 100% of the submissions which make the even a slight or partial match to any template in the system, there will be problems with legitimate users. Since the “actual” overall acceptance rate is known to reach only 90% in the example, the device will be incapable of matching ten users out of one hundred in the system. Some of those failures will be legitimate users; perhaps because the biometric is injured or changed, the sensor is dirty, or because the user’s template is of poor quality. If no match is made by a system that is set to 100% acceptance, the user is still rejected, whether she is a valid user or not.

In this example, the real world accuracy rate will be marginal and security nonexistent because anyone who is successfully scanned – anyone in the (real world delimited) 90% acceptance rate – and anyone whose scan matches the slightest portion of a template will be verified. However, the vendor's effective 90% acceptance rate sounds good to clients, and most users will not have to suffer through multiple scans or false rejection.

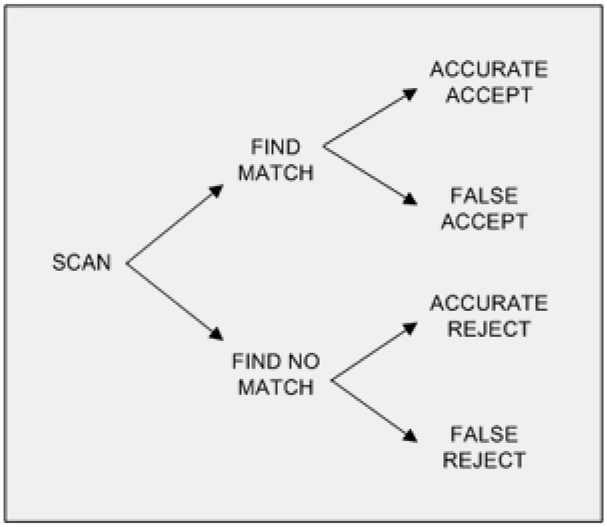

Figure 1. scan process tree

Next, false rejection and false acceptance are affected by adusting the system. In Figure 2., assume a vendor believes that he has achieved optimal performance and has these percentages after testing and adjusting the system. Although the false accept and reject rates are a mere 1%, assume that the vendor's client wants to further reduce false rejections. In this situation, the vendor can adjust the system by setting a higher initial acceptance, as shown in Figure 3. However, the situation has not really improved. Because the system is reducing the required score for a match or relaxing some other requirement, a match is now 4% more likely to occur on a given dataset. The false reject rate goes down and more users gain access. The false rejection rate drops to a client acceptable .5%. However, the 1% false accept rate is now 5%. In other words, another 4% of the access to the secured area or data is inappropriate. Such a tradeoff is an unacceptable solution.

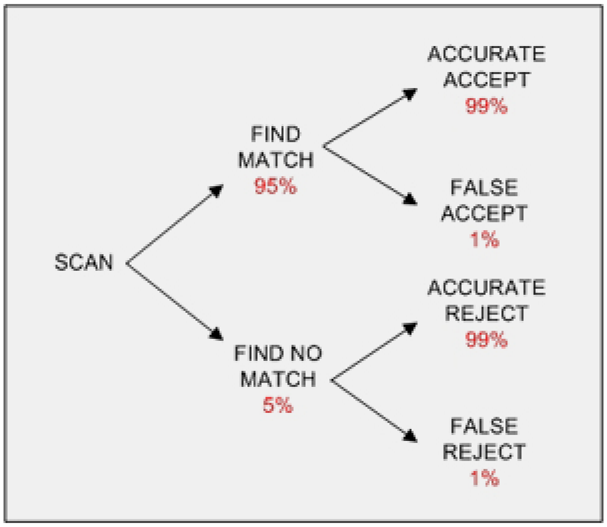

Figure 2.

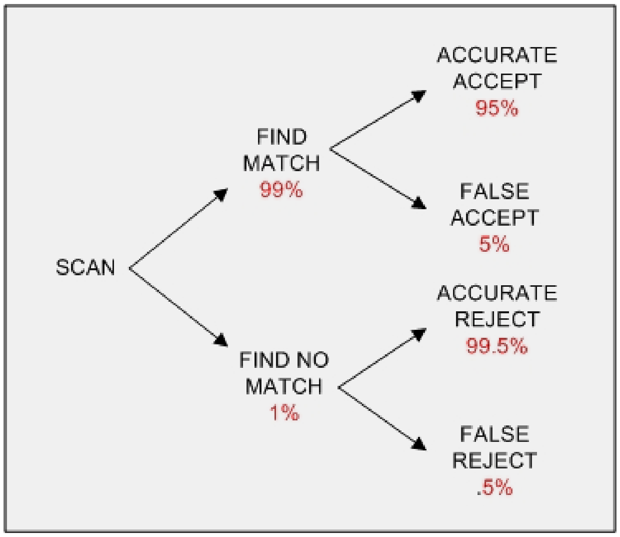

Figure 3.

In response to the rise in false accepts, the vendor scurries to adjust for the new flaw because the client insists on as little false acceptance as possible. As shown in Figure 4., the scales have now tipped the other way. Now, one hundredth of a percent of the validation process is granting inappropriate access. But mathematically, in order to accomplish this, 15% of users that should be accepted have to be rejected as well.

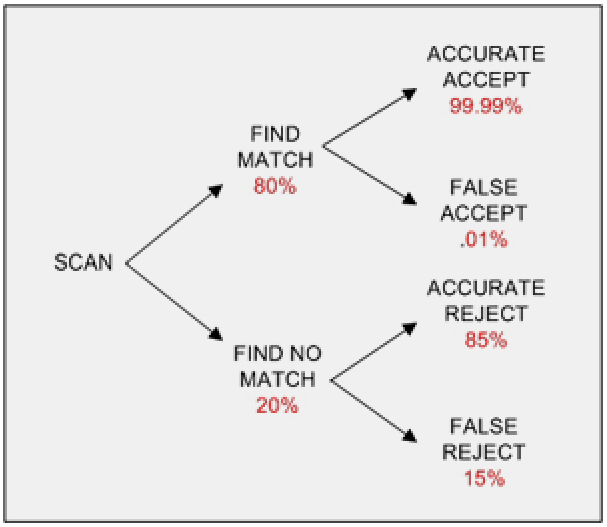

Figure 4.

The above example is one way that vendors can adjust their systems, but it reveals the critical flaw in the technology – once a combination of hardware and software yields a measured ability to handle input, that input can only be loosened or tightened, and one side of the equation suffers. It becomes a zero sum situation. As the National Institute of Standards and Technology (NIST) points out in their publication, *Standards for Biometric Accuracy, Tamper Resistance, and Interoperability*, "there is a trade-off between these two tasks, and one cannot simultaneously maximize the performance of both tasks [18]." In light of this, manufacturer accuracy rates may not be trustworthy. Vendors have a monetary incentive to adjust and to report statistics to their advantage.

Ideal rates are often achievable only under the manufacturer’s optimal laboratory conditions, which may be a clean room with perfect lighting and very clean submissions; lighting, dust particles, skin oils, skin and air moisture levels, ambient temperature, noisy sensor data, and many other variables all affect scans [19]. A “bad” scan can happen even at a theoretical 99% accuracy rate. Optimal conditions do not exist, and since vendors can skew the results in their favor, anyone considering the implementation of a biometric scanning system must investigate diligently what happens in a production environment.

Scalability

One of the greatest advantages of biometrics is that they are almost entirely unique. They are not *completely* unique, however. Although unlikely that two individuals with identical fingerprints would end up accessing the same system, conventional wisdom is flawed when it assumes that fingerprints are 100% unique. No statistical evidence exists to prove that all fingerprints are unique [20]. There is current disagreement among experts regarding the number of minutiae, or points of match, that are sufficient to make a positive match with certainty. One problem is that the federal and state databases that hold fingerprints are vast and growing rapidly [20]. In 2003, an American lawyer was arrested for a crime committed by an Algerian because their fingerprints had 15 points of match in common [20]. Eight points of match are used regularly to convict the accused, and the FBI is on record stating that the evidence in this case was “absolutely incontrovertible [20]”.

So, although only very small probability exists that someone may eventually scan as someone else if biometric scanners do not score enough minutiae, it leads to a larger point. Fingerprinting, a biometric system trusted for decades and believed to be foolproof, is preparing to break new ground with statistical research for validation or refute [20]. Simultaneously, new technology that relies upon the uniqueness of fingerprints has arrived with claims that it solves security problems. According to University of Virginia law professor and Harvard University visiting Professor, Jennifer Mnookin [20], there is no consensus about how many points of match can definitively determine a match. If Mnookin's claim is true, biometric device manufacturers, who must use either existing match scales or ones of their own creation, are unrealistic in any expectation of manufacturing products which are statistically accurate on very large scales. A NIST study concluded that a database of 40 million people would require four fingers to make a match without finding duplicates [18].

Success rates in matching ability vary greatly from device to device. NIST concluded that for a "database size of 1000 subjects, the rank one identification accuracy of a single finger is 93% while the rank one identification accuracy for a face is 83% [18]." The NIST summary defines "rank one" as the match that scores the highest score after the entire database is scored against a particular entry. The NIST study also notes a 1% chance of false acceptance for a database of 6000 fingers or 3000 faces. Both estimates assume optimal lighting conditions. In another study, NIST found that verification performance – just recognizing the face at all – drops from 95% indoors to 54% with outdoor lighting for the *best* facial recognition system [21]. The low accuracy rating means frustration for users, because they will be falsely rejected by the system. Biometric technology will undoubtedly improve over time. At this point, however, large scale biometric databases are technologically infeasible.

Identification versus Authentication

There exists a subtle but important distinction between identification and authentication (sometimes referred to as verification). Identification is a process of matching an individual against an entire database for a given purpose, without the necessity of an identity claim by the individual [22]. Identification asks the question: who are you? Authentication is a one-to-one matching process, where who someone claims to be is matched against a single record in a database [22]. Authentication asks: are you who you say you are? In the situation of a computer login, the username is the identification and the password is the authentication. When using a biometric scanner, the username and password are combined as a single entity, which is both an advantage and a danger of biometric systems. An important question that arises is whether or not combining identification and authentication is an improvement in security. A benefit of biomtric technology is that it is possible to authenticate a biometric against a database without ever identifying the person. Think of a fingerprint as a password that is assumed so unique that it provides access based solely on the approval of that biometric "password" with no "username" required. The tradeoff is that the username and password (or identifier and authenticator) are permanently tied together, which means that linking the identifier to the authenticator could be done without the knowledge of the person who supplied it. This problem is certain to generate privacy concerns in the future because if the system owner desires, this action can be done at any point in time after the biometric is collected.

Temporal Nature

Biometrics have a temporal quality that is regularly discussed in publications. Aging and growth cause our skin texture and placement to shift. Furthermore, damage to the dermis can alter the presentation of skin-based biometrics [23]. This creates a problem that will become a bigger issue as the technology pervades. Sensor designs must either adjust for age, possibly increasing false positives in the process, or re-enrollment may be required every few years. *The NIST Face Recognition Vendor Test 2002* found that even the top three tested systems identified 18 to 22 year olds 12% less reliably than 38 to 42 year olds, at 62% and 74%, respectively [21].

Irreplaceability

The irreplaceability of biometrics is perhaps the biggest roadblock to their widespread adoption. As previously noted, no one can reissue a biometric should it be stolen or copied. This is a fundamental point that detracts from the position of anyone who argues that giving a biometric scan is no different than giving your social security number. Besides the fact that a SSN is revealed selectively and with relative caution by most knowledgeable persons, if it is stolen, it is still possible (albeit difficult) to get a replacement. Security precautions exist for the protection of SSNs. For example, watch lists at credit agencies detect new accounts being opened using pilfered SSNs. In contrast, biometrics companies have no known security precautions or agencies to protect this irreplaceable commodity.

DEFEATING ATTACKS

Development and testing standards should be created to assist in the deterrence of many of the attack methods discussed. Although one manufacturer may block one attack effectively, another may not. Open standards would create an opportunity for manufacturers to contribute to the improvement of all similar devices. However, open standards are often not embraced by corporations because of the perceived notion that they can work against a company that wants to set itself apart as a market leader who manufactures a superior product. On the other hand, proprietary industry standards would require a standards body. This arrangement has its own set of issues to consider but are beyond the scope of this discussion. Nevertheless, if manufacturers in industries that deal with government regulations and industry standards for things such as electronic equipment, material usage and handling, etc., can find ways to create a body of standards with a governing body to provide oversight, there is no reason why biometric technologies should be any different. Adherence to open standards or having a governing body to provide oversight would make using biometric technologies safer for all.

Jain and Ulidag [24] suggest that encryption, watermarking, and steganography could be used to protect against biometric attacks. Specifically, they suggest that data could be transmitted securely by hiding it in the electronic carrier between the scanner and the template-matching algorithms. Man in the middle attacks would then be rendered much more difficult to perpetrate, provided that an individual who successfully intercepts the transmission is unable to break the encryption scheme. The relative level of difficulty between interception and encryption breaking is substantial – enough to warrant further investigation into this method.

To further thwart the MITM threat, Ratha et al.[25] suggest a challenge/response system that requires an intelligent sensor to perform some mathematical task on a biometric scan which is then replicated at the backend. These challenge/response calculations must match on both ends and would theoretically remove the likelihood of a MITM insertion.

Hill-climbing attacks may be prevented by allowing a limited number of sequential attempts that do not produce a positive match [14]. Although this defensive technique has been defeated, the BioAPI Consortium still recommends such quantizing of the score for increased security against hill-climbing [15, 16]. Soutar [14] suggests "forced mutual authentication" between the device application and the backend system or through a third party verification component. The theory behind this type of authentication is that by forcing the device application and backend to recognize and to acknowledge each another in some way, another barrier is created against forgery.

Van der Putte and Keuning [26] discuss the possibility that heartbeat or blood pressure measurements could deter replay attacks, but they are ambivalent as to the feasibility of such measures. No existing liveness tests are undefeatable, and the technology to detect a replay attack is severely lacking [13]. Since replay attacks are such a simple attack type to replicate, finding a way to deter them is a critical area for future development and research.

There are no countermeasures for forced action attacks beyond typical self-defense and protection strategies such as awareness of personal surroundings, daylight, crowds, knowing a martial art, etc. The problem, as Schneier [9] points out, is that “while a biometric might be a unique identifier, it is not a secret.” Other researchers agree that the lack of secrecy is a serious problem [27]; our biometrics are not even well hidden. Credit cards and valuables can be left at home or hidden, but our fingers, eyes, and hand geometry are always in a known location and in plain view, tempting a would-be thief. Furthermore, fingerprints, DNA, and sweat are residual – they can be collected long after someone has left an area. The risk of biometric removal, forced presentation, latent theft and forgery are all dangerous problems that must be addressed.

Schneier [5] recommends the use of a PIN or password coupled with the biometric device. Such a solution would resolve the authentication versus identification issues, but the pairing of a password or PIN with a biometric, as many implementations do, is less that ideal because it does not absolve the user from the need to recall something. Thus, it does not necessarily make things easier when compared to traditional username and password systems. If people come to believe that the biometrics alone provide a secure solution, they will reject the reduction in user friendliness that additions such as passwords or PINs necessitate.

Another potential attack countermeasure is under current investigation. “Soft biometric” traits, such as gender, height, weight, hair, eye, or skin color, have shown to improve fingerprint scanner performance by up to 6% [19]. It is possible that such research will result in new and more secure biometric devices.

DISCUSSION OF BIOMETRICS OUTLOOK

There are many uses for biometrics, and one potential application that has made substantial headlines since the 9/11 attacks is using them to reduce identity theft because they purportedly guarantee identity. In the long term, there are certain to be complications and caveats that were not envisioned. It is possible that widespread use of an unregulated technology may actually enable a type of identity theft that is immeasurably more difficult to deter and to resolve as compared to today’s identity theft cases. For example, it will be difficult for someone to argue that their face/finger/palm/retina was not used to open an account that was validated by a biometric. Add a social security number and a mother’s maiden name to the biometric theft, and there is little recourse against a thief’s actions.

As of July 2004, if a US citizen is willing to give the U.S. Government a copy of his iris and fingerprint, and upon clearing a background and terrorist watch list check, that individual will receive a Registered Traveler card from the Transportation Security Administration [28]. This federal program, still in testing, allows a passenger faster movement through security checks at an airport via an automated kiosk. Not only is the government’s trust in biometrics very high in this program, but the people using the program are voluntarily providing the U.S. Government access to their iris scan and fingerprints for life.

Biometric standards are struggling to acheive broader support. Three specifications exist that are worthy of note. The BioAPI Consortium, which includes members such as Intel and HP (but not Microsoft or IBM) has created the BioAPI specification, which has remained without update at version 1.1 since March 2001. No current or future scheduled meetings were listed on the bioapi.org website as of 11/02/04.

NIST and the Biometric Consortium, under partial sponsorship from the National Security Agency, developed The Common Biometric Exchange File Format (CBEFF), which standardizes a file format to facilitate the "exchange and interoperability of biometric data [29]". This appears to be one of the more promising standards, although their is little evidence of an ongoing evolution of the standard.

The X9F4 working group is working to restrict access to biometric templates [30]. One of the standards to restrict that access, ANSI X9.84, failed to become an ISO standard after fast-track submission in 2001 [31]. The current status of this standard is unknown, but as with CBEFF, there is little evidence of an ongoing evolution.

There are several other industry-specific and industry-related standards groups and trade associations, including the International Biometric Industry Association (IBIA), the M1 technical committee, the InterNational Committee for Information Technology Standards, and those mentioned previously such as the Biometric Consortium, the BioAPI Consortium, NIST, the ISO, and ANSI. Nevertheless, regulatory standards bodies specific to the growing biometrics industry do not presently exist to provide oversight of the technology.

Biometric technologies should not necessarily be condemned just because they carry risks. Current authentication methods are inherently problematic. Most people occasionally forget one or more of their passwords, do not rotate their passwords often or at all, use simple passwords, or are in danger of social engineering exploits. Reliance on biometrics to solve password woes is not currently a viable solution when so many problems and potential threats exist with their use.

Biometric technology solutions have emerged from rational minds searching for solutions to the problems of current data protection measures. Although biometrics have been around in various forms since the dawn of mankind, the current technological form is nascent. Rational consideration must be given to the long-term security and privacy issues created when biometrics are used. As information professionals, we must not allow a giddy consumer interest or a “wow effect” to override our responsibility to inform and to educate. If, as a community, we allow biometric ubiquity without profound and outspoken consideration of these issues and risks, we do a disservice to our fellow citizens, our progeny, and ourselves.

ACKNOWLEDGEMENTS

I would like to thank the advice of my advisor and friend Jeannie Walsh, for her insights into holding the reader’s attention by choosing the right words. If this paper is well written, it’s because she made sure that I made sense. I would also like to thank Ben Brunk, a friend and colleague who’s insights into biometrics did nothing but make this paper stronger than its original form. Without his input, I would have dropped the proverbial ball in a few places. Thanks also to my mom for letting me bore her repeatedly with discussions of biometric risks late at night. Finally, and most importantly, thanks to my wife Hannah and my daughter Lauren for allowing me the hours away to get this paper researched and written.

CITED WORKS

[1] K. Mulady, “Grocer puts new way to pay at shoppers' fingertips,” *Seattle Post-Intelligencer Reporter,* 2 May 2004; http://seattlepi.nwsource.com/business/68789_finger02.asp.

[2] L. Mearian, “System break-in nets hackers 8 million credit card numbers,” *Computerworld*, 24 Feb 2003; http://www.computerworld.com/securitytopics/security/story/0,10801,78747,00.html.

[3] “Recovering From Identity Theft,” tech. report, *Federal Trade Commission*. http://www.consumer.gov/idtheft/recovering_idt.html.

[4] J. Vacca, “Biometric Security Solutions,” *Informit*, 25 October 2002; http://www.informit.com/isapi/product_id~%7BC3A2803B-7E73-4341-AB9F-BC91D275E970%7D/content/index.asp.

[5] B. Schneier, *Secrets and Lies, Digital Security in a Networked World*, New York: Wiley Computer Publishing, 2000.

[6] M. Jewell, “Database culture ripe for ID theft,” *Oakland Tribune*, 10 Aug 2004; http://www.oaklandtribune.com/Stories/0,1413,82~10834~2325047,00.html.

[7] J. Clothier, “Biometrics to keep handbags safe,” *CNN*, 28 July 2004; http://www.cnn.com/2004/TECH/07/26/biometrics.handbag/index.html.

[8] K. Maney, “Will that be cash, fingerprint or cellphone?” *USA Today*, Nov. 2003; pg. E.01; http://www.usatoday.com/tech/news/techinnovations/2003-11-17-bonus-cover_x.htm.

[9] B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York: Copernicus Books, 2003, pp.181-206.

[10] T. Matsumoto et al., “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems,” *Proc. SPIE, vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV*, 24-25 Jan 2002; http://dependability.cs.virginia.edu/bibliography/s5p4.pdf.

[11] “Fingerprint Identification Systems – Capacitive Sensors,” online memo, *Bergdata Biometrics GmbH,* http://www.bergdata.com/en/technology/capacitive.php.

[12] L. Thalheim, J. Krissler, and P. Ziegler, “Body Check: Biometric Access Protection Devices and their Programs Put to the Test,” *c’t*. Nov. 2002: 114; http://www.heise.de/ct/english/02/11/114/.[13] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," http://biometrics.cse.msu.edu/EI5306-62-manuscript.pdf.

[14] C. Soutar, “Biometric System Security,” tech. report, *bioscrypt*, 2002; http://www.bioscrypt.com/assets/security_soutar.pdf.

[15] A. Adler, “Images can be Regenerated From Quantized Biometric Match Score Data,” http://www.site.uottawa.ca/~adler/publications/2004/adler-2004-ccece-quantized-match-score.pdf.

[16] *BioAPI Specification 1.1*, BioAPI Consortium, 2001; http://www.bioapi.org/BIOAPI1.1.pdf.

[17] N.K. Ratha, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” *IBM Systems Journal,* v 40, n 3, 2001; p 614-634.

[18] NIST report to the United States Congress, “Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability.” Nov 2002; pp. 2,11, ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf.

[19] A.K. Jain, S.C. Dass, and K. Nandakumar, “Can soft biometric traits assist user recognition?” *Proc. SPIE Defense and Security Symposium*, Orlando, April 2004, http://biometrics.cse.msu.edu/JainDassNandakumar_SPIE04.pdf.

[20] J.L. Mnookin, “The Achilles’ Heel of Fingerprints,” *The Washington Post*, A27, 29 May 2004; http://www.washingtonpost.com/ac2/wp-dyn/A64711-2004May28?language=printer.

[21] P.J. Phillips et al., “FRVT 2002: Overview and Summary,” *NIST* March 2003; p.2, http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf.

[22] J. Asburn, “The Distinction Between Authentication and Identification,” *Avanti*, 2000; http://homepage.ntlworld.com/avanti/authenticate.html.

[23] U. Uludag and A.K. Jain, “Multimedia Content Protection via Biometrics-Based Encryption,” *Proc. 2003International Conference on Multimedia and Expo (ICME 2003)*; http://biometrics.cse.msu.edu/UludagJain-ICME2003.pdf.

[24] A.K. Jain and U. Uludag, “Hiding Fingerprint Minutiae in Images,” *Proc. Automatic Identification Advanced Technologies (AutoID 2002)*; http://biometrics.cse.msu.edu/autoid02-n35-jain-uludag.pdf.

[25] N.K. Ratha, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” *IBM Systems Journal,* v 40, n 3, 2001, pp. 614-634.

[26] T. Van der Putte and J. Keuning, “Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned,” *Proc. Fourth Working Conference on Smart Card Research and Advanced Applications*, pp. 289-303, Kluwer Academic Publishers, 2000; http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf.

[27] A.K. Jain et al., “Biometrics: A Grand Challenge,” *Proc. International Conference on Pattern Recognition, Cambridge, UK*, 2004; http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf.

[28] M. Graczyk, “Houston airport using fingerprints, eye scan in security test,” *USA Today*, Aug. 2004; http://www.usatoday.com/travel/news/2004-08-04-houston-trusted_x.htm?POE=TRVISVA.

[29] *NISTIR 6529, The Common Biometric Exchange File Format (CBEFF)*, Information Technology Laboratory, Jan 1, 2001; http://www.itl.nist.gov/div895/isis/bc/cbeff/CBEFF010301web.PDF.

[30] J. Stapleton and J. Markowitz, “ANSI X9.84: Biometric Management and Security for the Financial Services Industry,” Nov. 2000; http://www.jmarkowitz.com/downloads/X984.ppt.

[31] J. Stapleton, “American National Standard X9.84-2001 Biometric Information Management and Security.” *Proc. Biometric Consortium Conference*, Feb 13-15, 2002; http://www.itl.nist.gov/div895/isis/bc2001/FINAL_BCFEB02/FINAL_4_Final%20Jeff%20Stapleton%20Brief.pdf.