Biometric Indicators: An insecure replacement for passwords.

Daniel Meyerholt

Submitted to

MSIA Capstone Committee

Presented in Partial Fulfillment of the Requirements of the Masters of Information Assurance

Davenport University

March 2013
Abstract

The ability to automatically and positively identify an individual is quickly gaining popularity with many organizations. Organizations are looking to leverage biometric technology in a way that can improve convenience, satisfaction, security and ultimately profitability. The fact that biometric indicators can be easily and quickly measured is also the biggest threat to using biometric indicators as an authentication mechanism. This threat is the fact that many of the biometric indicators are not, and may be difficult to keep, a secret. Biometric technology has become popular because many claim that it is easy for authorized users to gain access while unauthorized users are denied access. Many biometric indicators, such as fingerprints, can be captured without any inconvenience to the user and can even be collected without the user’s knowledge or consent. This renders biometric indicators insecure as a replacement for passwords. Biometric indicators cannot be easily changed if they are compromised, lost or stolen.
Table of Contents

Abstract ........................................................................................................................................... 2

Table of Contents ............................................................................................................................ 3

Introduction ..................................................................................................................................... 4

Literature Review ............................................................................................................................ 5

SplashData's worst passwords ................................................................................................... 5
Epic failure of the online username/password system .............................................................. 6
The state of online passwords is absurd .................................................................................... 8
It's a nutty system ........................................................................................................................ 9
Biometric authentication as a more secure alternative to passwords. .................................... 13

Discussion ..................................................................................................................................... 16

Are biometric indicators unique? .............................................................................................. 17
Are biometric indicators permanent? ........................................................................................ 19
Are biometric indicators secret? .................................................................................................. 20

Conclusion and Recommendation .............................................................................................. 25

References ..................................................................................................................................... 27
**Introduction**

The ability to automatically and positively identify an individual is quickly gaining popularity with many organizations. Organizations are looking to leverage biometric technology in a way that can improve convenience, satisfaction, security and ultimately profitability. Some organizations such as theme parks can use biometric technology in the form of fingerprint readers to make it easier for authorized guests to re-enter theme parks while reducing ticket fraud by preventing unauthorized use of theme park tickets. Other organizations such as casinos can use biometric technology in the form of facial recognition to improve customer loyalty programs while reducing casino risks by identifying card counters, cheaters and even gambling addicts.

Government organizations can use biometric technology in many forms for many purposes including, but not limited to, identification cards, benefits program fraud prevention, background checks, passenger screening, suspect identification, and visitor tracking.

Each of these previously mentioned uses is a form of user identification. These uses allow the organization to identify people by matching the biometric indicator to a previously provided biometric indicator to verify that the person is who they claim to be.

Biometric indicators are the features that are expected to be unique to a single person. Biometric indicators are either physiological or behavioral. Physiological biometric indicators can include deoxyribonucleic acid (DNA), facial features, fingerprints, iris, voice, hand geometry, as well as any other measurable physical trait.

Behavioral biometric indicators include gait, speech patterns, typing patterns, as well as any other measurable behavioral trait. Many of the biometric indicators are easily and quickly measured without presenting much, if any, inconvenience to the user.
The fact that biometric indicators can be easily and quickly captured and measured is also the biggest threat to using biometric indicators as an authentication mechanism. This threat is the fact that many of the biometric indicators are not secret. Because many of the biometric indicators can be captured and measured without any inconvenience to the user it becomes rather easy for these biometric indicators to be captured and measured without the users’ knowledge or consent. Biometric indicators are not a secure replacement for passwords.

**Literature Review**

There is a plethora of literature that exists on the subject of biometrics. The literature is generally focused on how automated biometric technology can be leveraged to provide authentication or identification. It should be noted that authentication is generally used to determine if an individual is who they claim to be while identification is generally used to determine who an individual is from a group of known individuals.

The first area of literature that needs to be addressed is the current state of passwords. The weakness that passwords can present is one of the driving forces behind the increasing use of biometric authentication. There have been many news headlines about weak and insecure passwords being cracked and published.

**SplashData’s worst passwords**

An example of published weak and insecure passwords is SplashData’s worst passwords. This top 25 list was compiled from files containing millions of stolen passwords posted online by hackers. The top three passwords, ‘password,’ ‘123456,’ and ‘12345678,’ remain unchanged from last year's list. New entries to this year's list include ‘welcome,’ ‘jesus,’ ‘ninja,’ ‘mustang,’ and ‘password1.’ SplashData releases this annual list in an effort to encourage the adoption of stronger passwords (2012).
Table 1. Adapted from SplashData’s “Worst Passwords of 2012” & SplashData’s “Worst Passwords of 2011.”

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>password</td>
<td>Unchanged</td>
<td>password</td>
</tr>
<tr>
<td>2</td>
<td>123456</td>
<td>Unchanged</td>
<td>123456</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>Unchanged</td>
<td>12345678</td>
</tr>
<tr>
<td>4</td>
<td>abc123</td>
<td>Up 1</td>
<td>qwerty</td>
</tr>
<tr>
<td>5</td>
<td>qwerty</td>
<td>Down 1</td>
<td>abc123</td>
</tr>
<tr>
<td>6</td>
<td>monkey</td>
<td>Unchanged</td>
<td>monkey</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
<td>Up 1</td>
<td>12345678</td>
</tr>
<tr>
<td>8</td>
<td>dragon</td>
<td>Up 2</td>
<td>letmein</td>
</tr>
<tr>
<td>9</td>
<td>111111</td>
<td>Up 3</td>
<td>trustno1</td>
</tr>
<tr>
<td>10</td>
<td>baseball</td>
<td>Up 1</td>
<td>dragon</td>
</tr>
<tr>
<td>11</td>
<td>iloveyou</td>
<td>Up 2</td>
<td>baseball</td>
</tr>
<tr>
<td>12</td>
<td>trustno1</td>
<td>Down 3</td>
<td>111111</td>
</tr>
<tr>
<td>13</td>
<td>1234567</td>
<td>Down 6</td>
<td>iloveyou</td>
</tr>
<tr>
<td>14</td>
<td>sunshine</td>
<td>Up 1</td>
<td>master</td>
</tr>
<tr>
<td>15</td>
<td>master</td>
<td>Down 1</td>
<td>sunshine</td>
</tr>
<tr>
<td>16</td>
<td>123123</td>
<td>Up 4</td>
<td>ashley</td>
</tr>
<tr>
<td>17</td>
<td>welcome</td>
<td>New</td>
<td>bailey</td>
</tr>
<tr>
<td>18</td>
<td>shadow</td>
<td>Up 1</td>
<td>passw0rd</td>
</tr>
<tr>
<td>19</td>
<td>ashley</td>
<td>Down 3</td>
<td>shadow</td>
</tr>
<tr>
<td>20</td>
<td>football</td>
<td>Up 5</td>
<td>123123</td>
</tr>
<tr>
<td>21</td>
<td>jesus</td>
<td>New</td>
<td>654321</td>
</tr>
<tr>
<td>22</td>
<td>michael</td>
<td>Up 2</td>
<td>superman</td>
</tr>
<tr>
<td>23</td>
<td>ninja</td>
<td>New</td>
<td>qazwsx</td>
</tr>
<tr>
<td>24</td>
<td>mustang</td>
<td>New</td>
<td>michael</td>
</tr>
<tr>
<td>25</td>
<td>password1</td>
<td>New</td>
<td>football</td>
</tr>
</tbody>
</table>

As we can see from comparing SplashData’s “Worst Passwords of 2012” and SplashData’s “Worst Passwords of 2011” lists many of the weak and insecure passwords of 2011 continued to be used in 2012. The fact that many different systems continue to allow the use of these weak and insecure passwords shows that the current password system is flawed.

**Epic failure of the online username/password system**

Some of the literature discussed flaws in the current password system. Newman (2012) discussed an epic failure of the online username/password system.
But there’s a bigger problem that Honan’s hack brings to light, and that’s how broken the username/password system has become. Every online service we use invites another security threat—a way for hackers to sniff out passwords or glean the information they need to reset an account elsewhere. As Honan himself notes ‘My experience leads me to believe that cloud-based systems need fundamentally different security measures. Password-based security mechanisms — which can be cracked, reset, and socially engineered — no longer suffice in the era of cloud computing.’

Even if you lock down your Google account with two-step authentication, and Apple and Amazon fix their weak points, there’s no guarantee another service won’t fail, especially when all of them are set up to accommodate forgotten passwords with forgiving recovery mechanisms. What we really need is a new way of verifying our identities online that doesn’t involve memorizing dozens of alphanumeric combinations, and doesn’t add layers of complexity for users.

Slowly, the tech world is coming around to this idea. Tim Bray, who previously worked as Google’s Android developer advocate, recently switched positions within the company to tackle online identity. ‘Usernames and passwords generally suck and obviously don’t scale to the Internet, so we need to do away with ’em soonest,’ Bray wrote in a blog post. In response, Daring Fireball’s John Gruber called online identity ‘one of the big problems to be solved for the industry over the next decade.’

That’s why we need better, more effortless ways to lock down our accounts. How this should happen, exactly, is where things get tricky.
Even with a major overhaul in how we identify ourselves online, hackers may still find workarounds. But in time, we may be able to enjoy a system that’s more convenient for everyone— and less prone to horror stories for the unfortunate few. (¶ 4-6, 10, 15)

Newman acknowledged that the current password system is broken and gave examples of other technology experts that agree. As Newman says, any replacement for the current password system will be difficult to design and implement. The first reason is that hackers are and always will be looking for ways to crack and circumvent authentication and other security methods. The second reason is that many people, like Newman, expect that the authentication scheme be both secure and convenient.

The state of online passwords is absurd

Another example of literature that discussed the flaws in the current password system is the article by Greengard (2013) who said the state of online passwords is absurd.

You know a system is broken when almost nobody can use it. This is currently the case with online passwords. The situation has deteriorated to the point of absurdity. Every day, there's an article somewhere warning individuals to avoid stupid passwords like 'password' or '123456.'

No question, these are really dumb passwords. But it’s not as stupid as the system we currently have in place. Consider: We all log into dozens or hundreds of sites every week and, theoretically, we're supposed to have a different password for each site. Worse, we're supposed to memorize all these passwords and change them periodically.

Right. [sic] And we're supposed to walk 10,000 steps a day and save a couple of million dollars for retirement.
Fortunately, there are password management programs and they work pretty well. For example, iPassword and Roboform can securely store passwords and automatically enter them at the right website. But this is a Band-Aid that only hides the problem. In reality, most consumers don't use these programs and, in an enterprise environment, a lot of people are extremely complacent about passwords.

Fact is, [sic] we need to address the problem from an entirely different direction. Several companies already provide two-factor authentication tools that work across platforms and browsers. Although some organizations have already adopted these systems for internal use, the technology is essentially useless for consumers visiting websites and logging into online accounts. (¶ 1-5)

Greengard argued that memorizing the many various passwords that a single person needs to manage is the prevalent issue with the current password system. Greengard stated that password management software is just a Band-Aid and that the actual solution is two-factor authentication.

**It's a nutty system**

A third example of literature that discussed the flaws of the current password system is the article by Swaby (2012) who describes the system as nutty.

Let's take a little tally of where we've found ourselves, shall we? Studies show that we log into some 10 sites a day. Places that hold our most important data, like Gmail, Dropbox, and our bank, might ask us to jump through two tiers of password hoops in order for them to ensure our online security. Overall we're asked to hold keys to 30-40 sites in order to read the news, access our email, or book a haircut. For each of these sites,
security analysts recommend using a unique string of 14-characters made up of letters, numbers, and special symbols. But remember: Computers are quick to guess dictionary words, your birth year, and numbers substituted for letters. No repeats allowed. Oh, and whatever you do, don't write anything down.

Who can possibly remember all those characters?

It's a nutty system, so we ignore it, spreading the five or six passwords that we can remember across every online interaction. But that's not a good solution. Connect our sites with shared login information, and we're risking enormous chunks of our online lives. As Steve Ragan, a journalist at The Tech Herald demonstrated in January, a free program and a $300 computer can crack more than 25,000 passwords in seven minutes. Perhaps XKCD said it best: ‘Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.’

The craziest thing is: We've known all along that our brains are not cut out for this. Researchers observed password fatigue in the earliest days of computing. In a 1979 study conducted by Bell Labs cryptologist Robert Morris and computer scientist Ken Thompson, the challenge was clear: ‘Human beings being what they are, there is a strong tendency for people to choose relatively short and simple passwords that they can remember. Given free choice, most people will choose their passwords from a restricted character set (e.g. all lower-case letters), and will often choose words or names.’

The researchers found that 60 percent of user passwords were less than 5 characters long, and overall, 86 percent relied on dictionaries or name lists to create them. Morris and Thompson concluded, ‘the results were disappointing, except to the bad guy.’
Sound familiar?

People have been crying, ‘the password is dead,’ for years (that one was courtesy of Bill Gates in 2004), but we're finally in a position where change is possible. When a keyboard was our only input, text passwords made sense, but now we have so many other entry points -- touch screens, cameras, microphones -- that are harder to replicate from afar. It might just be possible to create a login that doesn't sacrifice security for usability. So let's get on with it already.

The good news is, we've already started. Researchers are aiming for a new system that's not only human-compatible, but maybe even enjoyable, too. Take, for instance, the satisfying swipe. Touch-screen keyboards are annoying, but sliding your finger across a reactive surface at least initially caused a bit of a thrill. Android phones have taken this motion and applied it to a 3 x 3 grid login screen made of dots. Set up the phone with a pattern you fancy, repeat, and you're logged in.

Windows 8 has strengthened the idea by swapping the dots with a user's photo. By linking parts of the image that stand out (think: a mountain top, a sloth's nose) with lines, circles, and taps, you're actually telling the computer to remember a pattern dragged over a 10 x 10 grid. Work the same magic when you return, and you're in.

Touch-based operations get even more close to home. Nasir Memon, a professor of computer science engineering at NYU's Polytechnic Institute is taking our offline verification system, our signature, and making it an online one. His iPhone app, called iSignOn, learns your finger's path across the screen, unlocking when the shape and speed of the signature is repeated. The app is also a password manager, so once you're in, it will open the doors to a bunch of frequently used services.
The touch screen experience is breezy, but there are still problems. Android users, for instance, have expressed concern over ‘reverse smudge engineering.’ Because your finger traces a consistent pattern, the oils impart a trail that someone could follow to your data.

Memon estimates that iSignOn reaches about an 8-character password security equivalent. Still, he says, ‘A signature may come out differently if you're standing, sitting, or walking.’ So he's running trials, attempting to nail down the perfect mix of ease and rigor. ‘A four-digit password you enter only once. If I have to enter a gesture multiple times, I would not find that acceptable.’

In his quest for a better experience, Memon is also experimenting with biometrics on tablet devices. ‘Biometrics of the past required special equipment, which added to the cost. And besides, it was creepy. People don't like to feel that with their fingertips, their identity is being taken,’ he says. ‘Today it's different. The camera, the accelerometer, sensors--it's all there for you to use for free.’ What he's devised as a potential tablet login is a simple spin of a digital dial (the underlying engineering is anything but). Placing all five fingers on the screen gives the program data on the distance between your digits, their speed and shape as they spin, and their footprint -- not their fingerprint -- as they land on the surface. The information captured should eventually create a unique enough signature (it's at about six-character strength at the moment) to offer accurate access.

Are any of these approaches a panacea? Nope. Not even close. And as it stands, we've not yet nailed down a how many of these ideas measure up quantitatively. Getting them all to work together is considerably more daunting. Moreover, a system wide change will come at a staggering cost to businesses, so they'll resist it. And even once
we've scaled all these hurdles, real world tests like an attack on a biometrically protected Twitter account will surely take place. (¶ 3-15, 18)

Swaby discussed that a person’s memory is the major weakness of current password systems and gave the example of a study from 1979 that confirms that people prefer short and easy passwords. Swaby also discussed how touchscreen technology has allowed the use of swipe patterns to replace PINs and passwords, the new security challenges of swipe patterns and other challenges to future authentication systems.

**Biometric authentication as a more secure alternative to passwords.**

Rubens (2012) discusses biometric authentication as a more secure alternative to passwords.

Have passwords outlived their usefulness? Take a look at some of the weak passwords exposed in website breaches this year, and judge for yourself. The frequent usage of weak passwords such as ‘changeme,’ ‘123abc,’ and ‘Pa$$w0rd’ (real-life examples uncovered in the recent breach and defacement of a security software vendor’s website) are a strong indicator that enterprise organizations might be well-advised to consider a shift to new mechanisms for secure authentication that are more resistant to subversion by careless end-users.

Weak passwords are a problem because they are easy to guess – and they are certainly no match for brute-force password attacks by criminals using automated password cracking software such as John the Ripper.
One way to beef up the security of your authentication process is to force users to create long, complex passwords, but such enforcement comes at the risk of employees writing the passwords down – thereby defeating the attempt to increase security.

A better method is to adopt a two-factor authentication system. To authenticate, users have to supply a password (‘something they know’) as well as information from a second factor – typically ‘something they have,’ such as a one-time password generator token.

The Biometric Advantage

Of course, one-time password tokens can be lost as well as potentially hacked, so relying on ‘something they have’ is not always a foolproof approach.

Instead, an even more secure two-factor system can be based on ‘something they are’ – that is, biometric information derived from measurable biological or behavioral characteristics.

Common biological characteristics used for enterprise authentication are fingerprints, palm or finger vein patterns, iris features, and voice or face patterns. These last three involve no physical contact with a biometric sensor, which makes them less intrusive to use.

Behavioral characteristics such as keystroke dynamics – a measure of the way that a user types, analyzing features such as typing speed and the amount of time they ‘dwell’ on a given key – can also be used to authenticate a user.

The biggest growth area is the deployment of systems that make use of a smartphone as a portable biometric sensor, according to Ant Allan, a research vice president at Gartner. ‘There is an explosion in the choice of authentication methods open
to organizations, and we are certainly seeing a shift towards biometric systems that take advantage of sensors in mobile devices – the camera, for face or iris recognition, the microphone for voice recognition, and the keyboard for typing rhythm,’ he said.

The advantages of this smartphone-based approach are that it is not necessary to purchase any special biometric hardware, because users are likely to have their phone with them any time they need to log on to a system, and the phone's cellular or Wi-Fi connectivity can be used to transmit biometric information to a back-end authentication system.

Benefits and Drawbacks

The main benefit of using a biometric authentication factor instead of a physical token is that biometrics can't easily be lost, stolen, hacked, duplicated, or shared. They are also resistant to social engineering attacks – and since users are required to be present to use a biometric factor, it can also prevent unethical employees from repudiating responsibility for their actions by claiming an imposter had logged on using their authentication credentials when they were not present.

‘Biometric systems can be much more convenient than tokens and other systems, and are useful to augment existing security methods like passwords,’ said Alan Goode, a security analyst at Goode Intelligence. ‘For added security they are also sometimes used as a third factor,’ he added.

The main drawback of any biometric system is that it can never be 100 percent accurate. To use a biometric system, it is first necessary for each user to enroll by providing one or more samples of the biometric in question (such as a fingerprint) which is used to make a ‘template’ of that biometric. When a user attempts to authenticate, the
biometric they provide is then compared with their stored template. The system then assesses whether the sample is similar enough to the template to be judged to be a match.

A measure of a system's accuracy is commonly provided by two statistics: False Non Match Rate (FNMR) and False Match Rate (FMR). The former measures how often a biometric is not matched to the template when it should be, while the latter measures how often a false biometric is matched (and authentication is allowed) when it shouldn't be. Most biometric systems can be ‘tuned’ to reduce one of these two measurements, usually at the expense of the other. ‘It's important to understand that when a user supplies a password or a number from an OTP (one time password) token, it is either correct or it isn’t. With biometrics you never get a definitive yes or no,’ explained Mark Diodati, a Gartner analyst. (¶ 1-14)

As we can see with Rubens’ article biometric authentication is not an exact match but rather is measured for similarity to a stored template. We can also note that biometrics can be used as a supplement to the password system in order to provide multifactor authentication.

**Discussion**

Biometric technology has gained popularity because it appears that it is easier for authorized users to gain access while unauthorized users are denied access. With biometric technology it is trivial for an authorized user to use a fingerprint reader, facial recognition, or other biometric technology to gain access. The prevailing thought is that it should be impossible for an unauthorized user to gain access through the use of biometric technology.

This project challenges that idea with three questions that need to be discussed about biometric indicators.
The three questions are:

1. Are biometric indicators unique?
2. Are biometric indicators permanent?
3. Are biometric indicators secret?

The answers to these questions will show that biometric indicators are not a replacement for passwords.

**Are biometric indicators unique?**

For a biometric indicator to be useful for either authentication or identification the biometric indicator needs to be unique to a single person. The fingerprint is one of the most widely used biometric indicators. It is generally accepted that no two fingerprints are identical. There is little empirical evidence to prove that fingerprints are truly unique. However there is evidence of the shortcomings of fingerprint matching. Pankanti, Prabhakar, and Jain (2002) discuss the individuality of fingerprints.

The notion of fingerprint individuality has been widely accepted based on a manual inspection (by experts) of millions of fingerprints. However, the underlying scientific basis of fingerprint individuality has not been rigorously studied or tested. In March 2000, the US Department of Justice admitted that no such testing has been done and acknowledged the need for such a study.

What do we mean by fingerprint individuality? If two fingerprints originating from two different fingers are examined at a very high level of detail (resolution), we may find that the fingerprints are indeed different. However, most human experts and automatic fingerprint identification systems (AFIS) declare that the fingerprints originate
from the same source if they are ‘sufficiently’ similar. How similar should the two
fingerprints be before we can claim that they are from the same finger? This notion of
similarity depends on the typical (intra-class) variations observed in the multiple
impressions of a finger.

Fingerprints can be represented by a large number of features, including the
overall ridge flow pattern, ridge frequency, location and position of singular points
(core(s) and delta(s)), type, direction, and location of minutiae points, ridge counts
between pairs of minutiae, and location of pores. All these features contribute to
fingerprint individuality. (pp. 1-2)

Figure 1. Two fingerprint impressions from the same finger may look
significantly different (large intra-class variation). (Pankanti, Prabhakar, & Jain,
2002, p.2)

Figure 2. Two fingerprint impressions from different fingers may look similar to
an untrained eye (small interclass variation). (Pankanti, Prabhakar, & Jain, 2002,
p.2)
As we can see from the previous findings it does not actually matter if biometric indicators are truly unique. This is because the systems, and even the experts, determine the similarity of the biometric indicator by determining the number of corresponding minutiae. The uniqueness of biometric indicators to a specific system ultimately depends on the rate of false positives (unauthorized access allowed) and the rate of false negatives (authorized access denied) of that specific system.

**Are biometric indicators permanent?**

For a biometric indicator to be useful for either authentication or identification the biometric indicator also needs to be permanent. It is generally accepted that the fingerprints have a high level of permanence normally lasting from before birth until after death.
“Fingerprints are fully formed (i.e. became stable) at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual, except in case of accidents such as cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier” (Maltoni & Cappelli, 2008, p. 23).

“Fingerprints begin forming during the 12th week of gestation, and barring surgical or accidental removal of the finger itself, will remain permanent for the life of the individual until the body decomposes after death” (Crime Scene Forensics LLC, 2012, ¶ 1).

“Fingerprints are formed before birth, and while they grow larger throughout a person’s life, their basic structure remains constant. They can be temporarily obscured when the skin is damaged; but once healed, the ridges grow back in the exact same pattern. Even when a fingerprint is permanently scarred, there is almost always sufficient detail around the scar to allow for a positive identification” (King County Sheriff, 2012, ¶ 2).

While the ridges, valleys and features that construct fingerprints are permanent and can regenerate there are other factors that can obfuscate fingerprints. These factors include dirt and grime, touch pressure variance, dry skin, excessive moisture, medical conditions, etc. These factors do not permanently alter the fingerprint however they can make the collection and comparison of fingerprints difficult.

**Are biometric indicators secret?**

For a biometric indicator to be useful for authentication the biometric indicator needs to be secret. For a biometric indicator to be useful for identification the biometric indicator needs to be readily detectable.
Many biometric indicators such as fingerprints are readily detectable because of the nature of these indicators. Fingerprints, as well as palm prints, are located on the skin on the palm side of the hand. This means that fingerprints and palm prints are left on anything that is touched. A threat to using fingerprints as authentication is that fingerprints can be recovered from many surfaces. Yamashita and French (2011) discuss developing fingerprints from various surfaces.

Correctly identifying the type of surface expected to bear a fingerprint is an important step toward successful development. Surfaces are generally separated into two classes: porous and nonporous. This separation is required to select the proper technique or reagent and the appropriate sequential order for processing. Porous substrates are generally absorbent and include materials like paper, cardboard, wood, and other forms of cellulose. Fingerprints deposited onto these media absorb into the substrate and are somewhat durable. Amino acid techniques are particularly useful here because the amino acids tend to remain stationary when absorbed and do not migrate.

Nonporous surfaces do not absorb. These surfaces repel moisture and often appear polished. They include glass, metal, plastics, lacquered or painted wood, and rubber.

Latent prints on these substrates are more susceptible to damage because the fingerprint residue resides on the outermost surface. Cyanoacrylate (CA), dye stains, powders, and vacuum metal deposition are usually the best choices to use on these surfaces.

A type of substrate that does not easily fit into the first two categories but should be mentioned is considered semiporous. Semiporous surfaces are characterized by their nature to both resist and absorb fingerprint residue. Fingerprint residue on these surfaces
may or may not soak in because of the absorbent properties of the substrate and the variable viscous properties of the fingerprint residue. These surfaces include glossy cardboard, glossy magazine covers, some finished wood, and some cellophane. Semiporous surfaces should be treated with processes intended for both nonporous and porous surfaces.

Textured substrates can be porous or nonporous and present the problem of incomplete contact between the friction ridge skin and the surface being touched. (An example might be the pebbled plastic of some computer monitors.) This often results in fingerprints being discontinuous and lacking fine detail when developed. Additionally, these surfaces often do not respond well to a conventional brush and powder. The brushing action and tape lift typically develop the texture of the substrate, leaving fingerprints difficult or impossible to visualize. Various techniques, such as the use of very fine powder or flexible lifting media, may be used to reduce the problems caused by textured surfaces. (pp. 4-5).

Biometric databases also pose a threat to biometric indicators. These databases can contain large amounts of data such as biometric and other personal information that, if breached, can be utilized to circumvent biometric authentication. Ungerleider (2011) discusses the theft of a large government database as well as other countries that have or are building similar large databases.

Every time a foreigner comes to the United States, their biometric data--fingerprints and photographs--are processed into a massive database called US-VISIT. The service prevents identity fraud and helps find criminals, and countries all over the world have
adopted similar systems. Now Israel's has been hacked, leading to the leak of personal information of nearly every single citizen there (even some dead ones) onto the Internet.

Authorities in the Middle Eastern country announced the arrest on Monday of a suspect responsible for the massive data theft. He's a contract worker at the Israeli Welfare Ministry who was allegedly engaged in small-scale white collar crimes after-hours and who is accused of stealing Israel's primary national biometric database in 2006. He had access to the database, which is part of the country's population registry, through his office.

The stolen database contained the name, date of birth, national identification number, and family members of 9 million Israelis, living and dead. More alarmingly, the database contained information on the birth parents of hundreds of thousands of adopted Israelis--including children--and detailed health information on individual citizens.

There's only one problem: Biometric databases are the future. The Indian government is building the world's largest biometric database, which will handle the personal information of nearly 1 billion citizens and give millions easy access to health care and education. Many European Union members such as Germany and the Netherlands automatically include biometric information on passport RFID chips. Here in the United States, the FBI is building a billion-dollar biometric database that will give every single police department and sheriff's office in the country instant access to millions of mugshots and fingerprints.

In the Israeli case, a valuable database was stolen through an inside job. Although the information was stolen by a white-collar criminal with an identity theft jones [sic]
rather than by a hostile intelligence service or an enemy hacker, the end effect was the same.

The Federal Bureau of Investigation and the Department of Homeland Security have been less than forthcoming about efforts to secure the data contained in their respective biometric databases. However, a DHS privacy impact assessment conducted for the Coast Guard's ‘Biometrics at Sea’ program found numerous privacy concerns and weak spots that required additional security. Both the FBI and Homeland Security's databases will retain decades' worth of personal information, photographs, and fingerprints.

In the end, the government--and taxpayers--have chosen the efficiency and cost savings of biometric databases over the privacy and civil liberties concerns that experts have raised. But as the Israeli example shows, today's biometric database could easily become tomorrow's warez download. (¶ 1-3, 7-10)

Another threat to biometric indicators is not as highly technical as lifting fingerprints from various surfaces or pilfering large government databases. This threat is nontechnical and requires physical access to both the biometric indicator and the system to be compromised. Kent (2005) provided an example of a rubber-hose attack that occurred in Malaysia.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

The gang, armed with long machetes, demanded the keys to his car.

The attackers forced Mr Kumaran to put his finger on the security panel to start the vehicle, bundled him into the back seat and drove off.
But having stripped the car, the thieves became frustrated when they wanted to restart it. They found they [sic] again could not bypass the immobiliser, which needs the owner’s fingerprint to disarm it.

They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete. (¶ 1-3, 5-7)

As we can see from the previous discussion, biometric indicators are not secret. Many biometric indicators, such as fingerprints, can be captured and measured without much inconvenience to the user. Biometric indicators can even be collected without the user’s knowledge or consent. Biometric indicators are also subject to rubber-hose attacks where the biometric indicator is forcibly used or even removed against the user’s will.

**Conclusion and Recommendation**

Biometric indicators are not a secure replacement for passwords. Using biometric indicators as a replacement for passwords would have the same effect on security as users leaving their passwords everywhere they visit. A person has a limited number of biometric indicators such as fingers, eyes, face, etc. Biometric indicators are not easily changed if they are compromised, lost or stolen.

It is generally accepted that biometric indicators are unique; however the individuality of biometric indicators is dependent upon the biometric system that is being used. It is generally accepted that biometric indicators are permanent; however there are medical conditions and environmental factors that can affect the use of certain biometric indicators. Biometric indicators can be collected without inconveniencing the user and can even be collected without the user’s knowledge or consent.
Biometric indicators are great for providing identification of an individual. Biometric indicators are also useful as a supplement to other user authentication methods where knowledge or duplication of the biometric indicator does not affect security.

Multifactor authentication is recommended to improve the security of a system above the level that passwords or biometrics can provide independently. Multifactor authentication requires an attacker to duplicate or gain knowledge of multiple factors making a successful security breach more difficult.
References

Crime Scene Forensics, LLC. (2012). *Fingerprints are permanent and individually unique.* (¶ 1).


Newman, J. (2012, August 8). *The username/password system is broken: Here are some ideas for fixing it.* (¶ 4-6, 10, 15). Retrieved from http://techland.time.com/2012/08/08/online-passwords-are-a-broken-system-here-are-some-ways-to-fix-it/


