Biometric Data: A Brief History, Analysis and Reflection

Maxwell Kizewski and Taylor Bauer

COM 450 - Network Defense and Security

Dr. Marwan Omar

March 5, 2019

Abstract

Biometric data is an emerging form of password security that is sweeping the world. Due to its efficiency and easy accessibility, biometrics have become an effective way to safeguard personal information. The overall concept behind biometric data is that it uses properties of an individual's body to validate identity. While these systems are very effective and easily accessible, there are definitive drawbacks that make this technology difficult to apply to every environment. For this reason, it is difficult to weigh the positive and negative attributes of this technology as each environment has different qualifications, but through research and documented interpretation we are able to better incline ourselves towards the realities of this technology. Through our research, we found that the overall necessity of the individual to understand before applying this technology into any environment is specifically understanding how it all works and where problems could potentially arise.

History

In order to better understand biometric data, it is imperative to first understand the historical elements of biometrics and how the technologies of today became as popular as they have. According to Harold Cummins of Northwestern University Law, there are several historical events where fingerprints have been used and earmarked as the first forms of biometric verification. In Babylonian excavations dated back to 586 BC, the remains of several fingerprints found embedded in clay pots that were used to identify that particular pots were created by the same potter. There are even Assyrian tablets that contained contracts in cuneiform that were "signed" with the use of a finger tip impressed into the clay (Cummins, 476-477). As time

progressed, it was noted that different Europeans eventually caught onto the idea that fingerprinting could be used as potential means of verifying individual identity. Dr. Nehemiah Grew found in 1684 that friction ridge skin was identified on peoples hands (Barnes, 9). It wasn't until 1788 that it was noticed by J.C.A. Mayer that this skin was completely unique for each individual and it wasn't until 1892 where Sir Francis Galton found out that all fingerprints were completely unique and individualized (Barnes, 13).

Fingerprinting Technologies

As earlier described, fingerprints have been some of the most understood methods of biometric identification that the world has ever encountered. Like the early Babylonians, fingerprints have been used as a means to properly identify and understand identity. Fingerprints have different styles and shapes, which makes them privileged targets when it comes to identification. For example, in the modern era the primary use of fingerprint technology is that of mobile devices. Fingerprints are an easily accessible means of identification that can be applied well because of their easy availability. These forms of technology have been able to fortify the market as they have been able to have positive market response, it does not mean that these systems are perfect.

In modern application, the essential elements of a good fingerprint scanner is that in which looks at the grooves of a finger tip and compares them to that of a given database. This particular database stores all of the biometric data for a company/organization, or is locally stored in a similar way to that of a mobile device. As according to Norton Technologies, the greatest threat to these types of systems is that biometric data must be stored on a server which

also needs to be properly protected. With the common nature of biometrics, like the fingerprint scanner, there is a likelihood that data could be carelessly stored on not very well protected servers and your data could be accessed (Symantec, 2018). This ultimately means that the more possible ways in which this data is incorporated, the more likely it is that the data can be stolen from low security areas. Likewise, a company has to store biometric data in a database, which can potentially be stolen and used to gain access to other areas. Clearly, this type of behavior could cause malicious acts to be conducted and therefore making this type of information extremely sensitive.

Although this is a general fear with all forms of biometric data, fingerprints are certainly the most vulnerable due to the fact that they are so much more easily accessible through phones and personal computers. The tech giants Samsung, Apple and Google have all incorporated the elements of fingerprinting into their phones. As this technology continues to grow, the more likely people's digital footprint will be accessible.

Facial Recognition and Other Biometric Methods

The other most common form of biometric data that is commonly used is facial recognition. Facial recognition is an emerging technology that is becoming more popular in a lot of phones and personal computers because of how basic it is to implement the software. According to Steve Symanovich from Norton, this type of authentication works in a three step process. The first step takes a picture of the individuals face. Then, an algorithm looks at the geometry of the individuals face and compares it to known faces in a database, It then tries to see if the geometric patterns line up with the individuals face that is trying to be authorized

(Symantec, 2018). However, it should be known that this technology is not only restricted by corporate or recreational use. The government has been very keen on using this technology in an effort of homeland security. According to the Department of State, ABIS (Automated Biometric Identification System) has been implemented in government surveillance in an effort to better monitor visas that are given to foreign nationals. This system has also been argued to be used by police departments as well to help prevent crime in certain areas domestically as well (Grafeld, 2008).

There are also other prevalent systems that are being implemented regularly as well, including retinal scans, iris scans, voice analysis and hand geometry. While all of these are valid forms of biometric data, these systems can be exploited potentially if there is dire malicious intent. If a particular database were breached holding this type of data, not only is it irreplaceable but it is also extremely easy to then replicate or spoof technology into believing that particular data is genuine even though it is not (this will be talked more in depth later in this essay). Likewise, systems like Amazon's Alexa are also integrated with voice recognition, allowing specific voice data to become the standard for specific commands, but is now being adapted to ensure that that data is specific per user based on behavioral analysis.

Risks and Analysis

The risk of cyber criminals being able to steal a users credentials is well known. Cyber criminals use extensive amounts of resources in order to commit these crimes. Along with using any new innovative ways to hack all the standard methods such as phishing, Trojans horses, malware even brute force still work just fine. A major issue why it is so easy to hack a users

password is because people make basic passwords and will continue to do so. No person wants to sit and memorize a random string of randomized numbers as their password.

There is a possible solution that is being worked on, behavioral biometrics. The idea may seem strange or a waste of time to some. However, there are an enormous amounts of studies that show that people behave in very unique ways. There are also many different ways this behavior could be analyzed. Some examples being, how fast we type our password, how hard we hit each key when typing, how fast we move our mouse cursor. These just being a few examples of how people operate their workstation.

One software development team worked on a software called SilentSense which used behavioral biometrics on Android Smartphones. Their software would determine how hard people were pressing on their screen and sensed key movements when operating the phone. The software operated completely in the background of the phone. Their results surprised most people “We conduct extensive evaluations of our approaches on the Android smartphone, we show that the user identification accuracy is over 99%” (Bo, Zhang,& Li, 2013). The issue that set the software back was it would never be able to stop running which consumed massive amounts of battery power.

This kind of solution if further explored can solve an enormous amount of cyber problems people are facing. This would reduce the size of bot networks dramatically, reduce the selling of private information, and reduce cyber crime in general. Other positives of exploring behavioral is there is no need for any special hardware. All the user needs is a keyboard and

mouse to function with the software. Also it requires no extra effort from the user which is what causes vulnerabilities in the first place.

Vulnerabilities in Fingerprint Biometrics

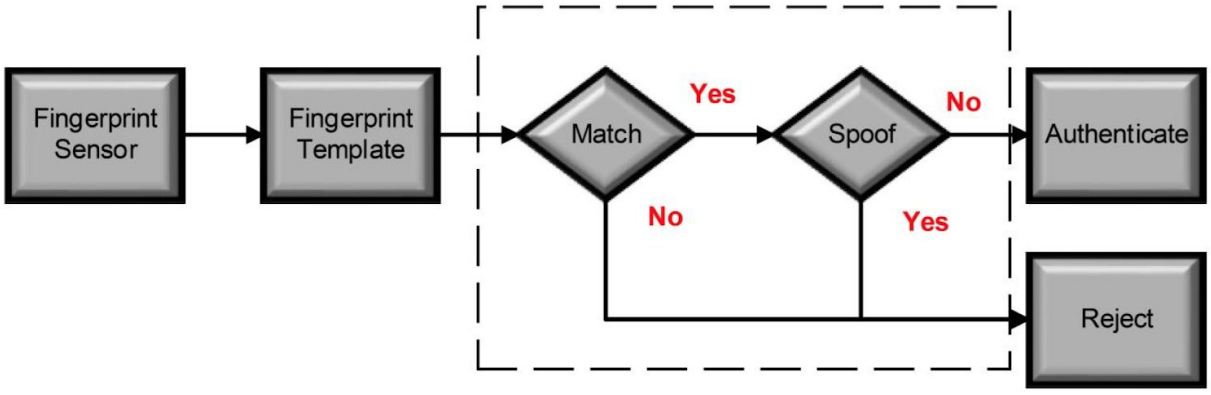
In many ways the use of biometrics is more convenient then traditionally typing in a password. Sadly, convenience often creates new security risks that can often be exploited. Ever since apple released an Iphone that had fingerprint authentication capabilities in 2013, fingerprint spoofing has become increasingly popular. There are several ways to hack into a device that requires a fingerprint.

In order for the machine to remember your fingerprint, that image must be stored into a database. Unfortunately, these databases are no different from others, it can still be hacked into. These databases that are holding images of your fingerprint are frequent targets. Since a person's fingerprint is considered confidential, there usually is other classified information such as a person social security number or personal passwords stored within the database. All this information is worth a great deal on the black market. The right persons finger print can sell for a substantial amount of money since he or she can't just go out and get a new fingerprint. These breaches are more common than most would typically think "A notorious breach in 2015 involved the electronic hack of a U.S. Office of Personnel Management database containing 21.5 million federal employee records. Among the records were some 5.6 million fingerprint images, including those from undercover agents." (Symantec, 2016).

This incident created a major security risk, many buildings require government officials to use their finger print and now since their fingerprint was leaked, government buildings were considered in potential danger.

The ultimate trend that is noticeable here is that most validation protocols are using a similar protocol as described in the Synaptics article concerning the safety of fingerprints. As depicted in the graphic below, a sensor brings in the data that is being authorized and compares it to the stored template of the authorized individual. If there is a match, it will verify it as a genuine match of the fingerprint and grant the user access or it will identify the match as a spoof and deny access. Otherwise, if the match does not line up, it rejects the attempt all together.

Although a physical hacks are much less tempting to an experienced hacker it's still a



major threat that should be taken seriously. It is extremely easy to create a fingerprint, now with tools like 3d printers becoming more accessible by the day the need for security grows. In some cases a hacker may not even need a 3d printer to craft the print. The process for re-creating the user's finger print is: scan the fingerprint in high resolution, print the image on to a mold or

using a 3d printer, and lastly use the mold to go cause trouble. The most challenging part is being able to find the person's fingerprint that is in detailed enough condition to scan. However with how many items we touch on a daily basis most items we come in contact with will contain a useable fingerprint.

Prevention in Fingerprint Biometrics

Taking the necessary steps to prevent a fingerprint hack can save companies from potential disaster. Electronic hacks were mentioned as a major vulnerability. Although it's not as convenient, setting up the fingerprint scanner to just authenticate locally can increase your organization's security dramatically. The upsides to this method is there wouldn't even be a database for the hacker to access since all the files would be set up through the device locally. The downside is if the device were to break, the files containing the user's finger prints would be lost as well. This means you would have to re-add all your employee's fingerprints to the new system.

To create an anti-spoofing sensor either the software on the sensor would have to be updated or the hardware of the sensor needs to be upgraded. The Transport Layer Security (TLS) protocol is often worked with in order to protect the scanner from a fake finger attack. This protocol encrypts all information that is being sent between the sensor and the host. Upgrading the actual sensor adds on some serious security. This is known as a match-in-sensor technology. It is when every single scan is automatically authenticated or denied on the spot. There is no communicating with a host or a network. Also, these upgraded scanners detect temperature to verify that the user is a live person and not just a piece of plato or plastic. The most major issue

with this method is the cost to incorporate this kind of technology. Also if you wanted to implement this technology into a mobile device, the scanner would require an extraordinary amount of power which would really decrease battery life. Sadly, most consumers would prefer battery life over security.

Sources:

Barnes, J. G. (n.d.). History. Retrieved March 3, 2019, from https://www.ncjrs.gov/pdffiles1/nij/225321.pdf

Grafeld, M. P. (2008, August 28). Automated Biometric Identification System. Retrieved February 24, 2019, from https://2001-2009.state.gov/documents/organization/109132.pdf

Harold Cummins (1941-1942). *Ancient Finger Prints in Clay*, 32 J. Crim. L. & Criminology 468. Retrieved February 24, 2019, from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=3083&context=jclc

Symantec Corporation. (n.d.). Biometrics and biometric data: What is it and is it secure? Retrieved February 28, 2019, from https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Synaptics. (2016). Protecting Against Fingerprint Spoofing in Mobile Devices. Retrieved February 24, 2019, from https://www.synaptics.com/sites/default/files/sentrypoint-anti-spoofing-wp.pdf

Bo, C., Zhang, L., & Li, X. (2013). *SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics*. Retrieved February 25, 2019, from https://arxiv.org/pdf/1309.0073.pdf

Symantec Corporation (2016) *Protecting Against Fingerprint Spoofing in Mobile Devices*. (2016). Retrieved February 25, 2019, from https://www.synaptics.com/sites/default/files/sentrypoint-anti-spoofing-wp.pdf.