BIOMETRIC AUTHENTICATION

Group 5

Alexander Hickey, Brittany Walsh, Spencer Dee, Aaron White, Brian Lam

Table of Contents

Executive Summary

Biometric security systems have long been an affordable way to provide security to any business. However, with the rampant spread and continuation of the COVID-19 pandemic, biometrics requiring physical contact are a threat to public safety. The major contributor to this threat is that of fingerprint readers.

Fingerprint readers are cheap, very effective, and easy to integrate into any facility. Unfortunately, they also require anybody needing access to physically touch the same scanner as every other user. As it is not feasible to clean them after every use, they should be replaced as soon as possible.

Of the easily available biometric replacements, there are voice authentication, iris scanners, and contactless fingerprint readers. Each with their own upsides and downsides. Though some have more serious downsides than others leading to them not being a good choice for many companies.

Contactless fingerprint readers, while seemingly a perfect answer to the issues of conventional fingerprint readers, are much less accurate. This can be partially avoided through the use of multiple fingers, but it is difficult to match the strength of its physical counterpart.

Voice recognition is the least recommended of our proposed options. This is due to the ease at which a voice may be faked, such as through recording someone's voice on the phone. While this option may be fine for low security businesses, it is extremely dangerous for use anywhere else.

Finally, we have iris scanners, which are nearly as accurate as fingerprint readers without requiring any sort of physical contact. The largest drawback of iris scanners is their cost, requiring a much higher upfront cost for the hardware compared to the fingerprint readers currently being used around the world. This increased cost is the main reason that iris scanners haven't become the norm as of yet.

For these reasons, the recommended biometrics system that should be used at companies requiring as much security as possible in the middle of a global pandemic is: the iris scanner. The initial cost that would be required of many businesses to switch over will be massive, but it will help with the safety of the workers.

Fingerprint Scanners

Fingerprint scanners are devices used to identify an individual by scanning his or her fingerprints. The human finger possesses a plethora of ridges, and every human being to ever exist has had, and will always, have a unique pattern. This is how fingerprint scanners work; they pick up the unique ridge-like patterns on our fingers that are perfectly unique to us, log the measurements of the distances between the gaps, and are able to identify us (Ali). According to Spiceworks Today, 57% of organizations are currently using fingerprint scanning technology, and use about 24% plan to implement either fingerprint scanning or facial recognition within the next two years.

For the identification process to work, fingerprint scanners utilize a microprocessor, either a CCD (charge-coupled device) or a CMOS (complementary metal-oxide semiconductor) as an image sensor. The image sensor then captures a digital photograph. After the photograph is generated, it is mechanically examined by the microprocessor, where the ridges of the fingerprint itself are separated from the whole image. The refined image is then encrypted using pattern-identical software. Once encryption takes place, it is compared to the image on file, and identifies the individual based on the congruency of the two patterns (Ali).

Fingerprint scanners are among the most popularly used biometrics in existence. Some examples of biometrics used in commercial products are laptops, desktop computers, and smartphones. Fingerprint configurations have the ability to keep the personal information on your laptop safe, especially if you lose it.

The more prominent use of the fingerprint scanner is in smartphones. Nowadays, many people hold a lot of personal information on their personal smartphones, information like phone numbers, personal pictures, notes, documents, passwords, online browsing data, and banking information. Sometimes, even social security numbers are stored on smartphones. A fingerprint configuration is a great way to ensure that this information does not end up in the wrong hands, and offer more protection than passcodes, which malicious actors can target and exploit (Ali).

The use of fingerprint scanners also pairs well with the use of mantraps. A mantrap is a small vestibule or enclosure with two doors, an entryway and an exit, designed to trap an

individual before he or she may be granted clearance to enter a vital location. Some mantraps utilize a security guard, but we will be discussing how mantraps play into the use of biometrics as a means for identification. Mantraps paired with fingerprint scanners or other types of biometrics typically use interlocking mechanisms as a means for restricted entrance and exit. The individual enters through the entry door, verifies his or her identity with a successful fingerprint match, and is granted access to exit the mantrap.

Although fingerprint scanners are a prominent and secure medium for biometric privacy and security, they are not completely reliable. Ways to get past fingerprint configurations do exist. Those with malicious intent may use transparent film to collect residual fingerprint patterns to copy the unique data associated with them, or can use 3D mildew systems that create copies of preserved fingerprints. Also, scanners can possibly malfunction and disallow a user proper identification or full access if the skin on the finger is wet, or if the scanner surface has become too dirty or dusty (Ali).

Even through the shortcoming of not providing a complete guarantee of privacy and effectiveness, fingerprint scanners still remain a safe and relatively reliable biometric to identify individuals. Fingerprint scanners are able to work as well as they do because of the non-ambiguity associated with unique fingerprints for every individual. Without the use of specialized tools, it is next to impossible to be fraudulently identified. However, in the wake of the COVID-19 pandemic, new ramifications for the use of fingerprint scanners have made themselves known. The risk of non-sanitized contact on the highly-trafficked surfaces on fingerprint scanners has gone up, meaning that the use of fingerprint scanners could be cause for a greater spread of illnesses, like COVID-19. Luckily, there are contactless solutions for biometric identity verification.

Contactless Fingerprint Scanner

The COVID-19 pandemic has clearly had a major impact on all of our lives, and specifically has had a major impact on the biometric industry. Many biometrics have suffered due to the spread of the virus, and specifically fingerprint readers have become very dangerous for employees to utilize. This fear among employees has led many companies to explore different options in terms of access controls, whether it be biometrics or even more archaic

methods. We have discussed many different alternatives to fingerprint scanners throughout this paper, but two specifically that we believe to be effective are contactless fingerprint scanners as well as palm vein readers.

One alternative to fingerprint scanners, are fingerprint scanners that don't utilize contact. These scanners are used by hovering a hand (or multiple) above a scanner and the user's identification is established. The security of these fingerprint scanners is known to be reliable for the most part. It is very hard to forge someone else's fingerprint in order to gain access, due to the fact that there is no contact between the finger and the sensor, so the fingerprint essentially can't be duplicated unless the entire system is compromised. Contactless fingerprint scanners are still a relatively new form of biometric authentication and more testing does need to be done in the field. Due to the relatively new establishment of these scanners, fingerprint scanners that utilize contact are considered much more effective and accurate than scanners that don't. A study done by the National Institute of Standards and Technology showed that contactless fingerprint scanners demonstrate "…60% to 70% accuracy." Clearly, this would not be an acceptable form of authentication for any business as it doesn't demonstrate a very high rate of success.

However, there is a way that companies could work around this, as using multiple fingers in these scanners improves the authentication accuracy immensely. In the same study done by the National Institute of Standards and Technology it shows that when multiple fingers are utilized in the contactless fingerprint scanners "One mobile app reached 95% accuracy, and other devices reached close to 90% accuracy." Clearly when multiple fingers are utilized in these contactless fingerprint scanners, they are much more effective. Although a 90% success rate is not acceptable for any business, as development continues on this technology the success rate will clearly increase. Also, it's important to note that these scanners very rarely incorrectly identify users, as the study done by the NIST states "All contactless devices produced low false positive rates…". Clearly, we've seen over the last couple of weeks, the COVID-19 pandemic could last a very long time, and with proper development contactless fingerprint scanners would be considered a very effective alternative to regular fingerprint scanners.

Iris and Retina Scanners

When considering contactless ways of authentication, iris and retina scanners are the top models to consider. Iris scanners measure the pattern within the pattern circle of your eye in order to authenticate identification. Retina scanning is another ocular based method of authentication but has a few differences. Although both methods are very unique to each human, retinal scanning measures tissue that is in the posterior portion of the eye while iris scanning measures cells within the front of the eye where light still reaches.

Iris scanners are considered one of the most effective methods of biometric authentication due to its stability and affordability. The iris is the colored circle within someone's eye; this part of the eye is not likely to change over time. Furthermore, this is a part of the eye that is very difficult to replicate.

Iris recognition is different from retina recognition because of the level of intrusiveness it requires. The retina is the third layer of the eye that provides light sensitivity. Iris recognition measures a very superficial part of the eye while retina recognition requires measurement of a deeper part of the eyeball. Still, both iris and retina scanners provide speedy results that are typically extremely accurate. The only difference in accuracy comes from the retina, as certain eye diseases can cause changes in the retina. Price wise, a low-end ocular scanner could ring in at about $200 while the high-end versions could be priced up to several thousand dollars each (Smith).

Palm Vein Scanner

Another form of contactless authentication that would effectively reduce the rate of contracting COVID-19 is the use of palm vein scanners. Palm vein scanners are used by using an infrared light that identifies the unique pattern on a user's palm, and they are contactless which would clearly reduce the risk of getting COVID-19. These scanners are extremely accurate in identifying the user correctly due to the large number of data points present on a person's palm. In fact, they are much more accurate than the contactless fingerprint scanners and are currently considered a better alternative. One example of this is shown through the biometric organization Keyo, who develops palm vein scanners. On their website Keyo claims that their

palm vein scanners have "…an accuracy advantage compared to other biometrics." In fact, they claim that their scanners have a false rejection rate of 0.01%, which they claim is "...260 times more accurate" than other forms of biometric authentication such as facial recognition. The accuracy of the palm vein scanners along with the positive hygienic factors makes a palm vein scanner a very viable alternative to fingerprint scanners.

Another big difference between this form of biometrics compared to others is that authentication is established through an internal source. The palm vein can't be forged, while other forms of biometrics such as voice recognition (through the use of a recording), or regular fingerprint scanners (use of tape), can easily be bypassed. This high level of security makes the palm vein scanner a very advanced form of biometrics.

The only negative aspect of these palm vein scanners is the cost. While palm vein scanners do have increased security and accuracy, the cost of the scanners themselves is slightly more than that of a fingerprint scanner. This may lead to some problems for business' in our current economic climate. With many businesses losing revenue at an alarming rate due to quarantine regulations, it may be tough to switch their entire access control system to a form of biometrics that is more expensive than their current one.

In conclusion, when it comes to the contactless hand biometric access controls both contactless fingerprint capture and palm vein scanners could be very viable options. However, due to the lack of accuracy and research that is involved with the contactless fingerprint scanners, one could objectively conclude that palm vein scanners would be the better alternative. In either scenario, biometrics can still be very effectively utilized during the COVID-19 pandemic, and the industry may even grow rather than falter.

Voice Authentication Systems

A different solution to consider as COVID-19 continues to be a legitimate threat are voice authentication security systems. There are two main approaches to voice authentication: text-independent and text-dependent. If a company would like the system to be text-independent means that the user will have his or her own passphrase and the system will authenticate essentially identify that a user is who he or she is based on their voice sample. Text-dependent means that every user has a predetermined passphrase and just speaking the

phrase can grant access to the area/system. Both are secure in their own way but have clear security flaws.

While text-independent voice authentication systems prove to be more convenient for the average user; it is not as secure as one might think. A simple recording of someone's voice has been shown to thwart systems like this. Software is increasingly making it easier to replicate an individual's voice. "Ben Fisher, CEO at Magic & Co., a technology consultancy in New York City, says it should generally not be trusted on its own. In addition to being susceptible to voice mimicry and disguise, voiceprints can be thwarted by simply recording someone saying a phrase (such as "open") and replaying that recording." These issues can be addressed with a few different solutions. One of these is as simple as hiring a security guard to ensure that people are not spoofing voices. Require the employee or user to surrender their electronics until the authentication is complete, get metal scanned, perform the voice authentication, and they'll be on their way. Of course, this forces the authentication process to become less hygienic, so many companies may opt to accompany their voice authentication system with an anti-spoofing software. These software are created with the intent to discern between a human voice and a synthesized voice. Anti-spoofing works by detecting "certain signal artifacts that are sometimes indistinguishable by a human ear created by Speech conversion, replay attacks, and TTS (Text to speech)."

Text-dependent authentication systems are much less secure for one reason alone: all an individual needs to do is find out what the passphrase is. The system is indiscriminate against voices and will grant access as long as the correct phrase is used. Meaning that the company's security exponentially weakens as the number of employees increase. With more employee's the chance of a security breach in the form of accidentally revealing the passphrase to an individual who is not part of the company increases. Depending on the size of your company, this is another variable that should be considered when choosing your biometric system of choice.

Voice authentication systems are as cheap as the software. The hardware does not need to be the most sophisticated; what matters most is the program that is being run. As biometric systems continue to become more widely adopted in the professional community, the price of

systems continue to fall. Voice authentication systems are the cheapest biometric system currently. Without any of the equipment the SDK (software development kit) for a software such as Neurotechnology's Verispeak is $339. Other providers will offer a subscription-base that will prove to be cheaper over a certain period of time, but more expensive in the long run.

Works Cited

Ali, Zehra. “Fingerprint Scanners: How Do They Work?” *United States Cybersecurity*, United States Cybersecurity Magazine, 22 Apr. 2019, www.uscybersecurity.net/fingerprint-scanners/.

“Are Mantraps Effective and Where Should They Be Used?” *Total Security Solutions*, Total Security Solutions, 24 Jan. 2020, www.tssbulletproof.com/blog/mantraps-for-access-control/.

Karlskin, Beau. "5 Reasons Why Palm Vein Scan is the Best Biometric." 4 December 2019. *keyo.co.* 21 June 2020.

National Institute of Standards and Technology. "NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech." 19 May 2020. *nist.gov.* 20 June 2020.

Tsai, Peter. “Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?” *The Spiceworks Community*, Spiceworks, 12 Mar. 2018, community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure.

Smith, A. (n.d.). How Much Does Biometric Access Control Cost? Retrieved July 04, 2020, from https://kompareit.com/business/security-compare-access-control-biometric-cost.html