Mayur Suresh

Professor Ola Ajaj

CSC 301

December 7, 2021

Biometrics

The nature of biometrics is a more secure authentication system which is a physical security feature which blocks out any unauthorized access. This basically means that biometrics is like a physical key which is unique key and would not let anything access it other than this specific physical key. Biometrics include fingerprint recognition, iris recognition, facial recognition, voice recognition, hand geometry, etc. Some of the biometrics authentication we see are those that lets everyone access their devices that range from mobile phone, tablets and PCs.

One type of biometric authentication we have seen the longest, which is the cheaper option and convenient is the fingerprint recognition software. We have seen these on our phones and tables now even the newer generation PCs have adopted this software.

Another biometric software which has seen more traction over the last 10 years is the facial recognition software. We have also seen this software in more expensive phones, tablets and with the new Windows-10 update we have seen a facial recognition software in this place. While there are more biometric authentication software other than the usual fingerprint and facial recognition, like iris, voice recognition and hand geometry they have not hit the public market.

The fingerprint recognition software collects data from a person’s finger which includes the measurement of a finger’s unique ridges and then takes the collected data use it to produce an image or a unique digital signature. The signature then is compared to many different signatures to see if it is the same and either accepts or rejects the signature.

There are many different types of fingerprint readers. Optical Readers are the least expensive one and the most common type of reader which is basically a digital camera that takes a visual image of a fingerprint. One disadvantage of using the Optical Reader is since is a camera it is prone to get dirty or makers and also very easy to fool, since it is basically a picture of a fingerprint.

Ultrasound Readers software is one of the newer fingerprint readers that use high frequency soundwaves to reach the outer layer of the skin, then read the fingerprint. Unlike the Optical Reader, the Ultrasound Readers is more secure because it uses soundwaves and dirt does not interfere with the reader. This is more sophisticated because unlike the other readers this does not collect fingerprint in the form of an image of just the outside layer of the print, but a more detailed one. But this reader is more expensive than most readers because of the accuracy and the difficulty to breach this reader unlike the Optical Reader.

Another popular reader is the Capacitive readers. This reader unlike the others has a very unique way of collecting the print data. This reader uses electrical currents to create an image of sorts of the fingerprint. These Capacitive readers are not as expensive as the Ultrasound readers but still in the mid-range in their pricing and are very popular and are seen in most phones and tablets. These are used in most technology today because this reader unlike the optical readers needs an actual fingerprint. So, tricks in movies which use a sort of sticky transparent sheet to copy a fingerprint and use it to fool security will not work.

Lastly another popular scanner is the Thermal readers. These readers collect data from the difference in the temperature from the tiny ridges and curves in the fingerprint. But this type of reader is the most expensive and the most energy consuming so these are not fit for the public market yet.

Overall, fingerprint scanners are the most reliable and common biometric because not only are they on the cheaper side but also are efficient and safe when used with the proper fingerprint readers like the Capacitive Reader. Fingerprint authentication, as everyone who owns a phone knows, is the primary type of security, while before the primary security was like a pattern recognition or a pin code. So, I think that this will be replaced by a more reliable biometric authentication because other than the security issue discussed above there are also physical problems like an accidental loss of fingers, the burning off the fingerprint itself and many other difficulties. Some of the more reliable biometric authentication is the Facial Recognition.

Facial recognition is one of the most common biometric authentications that even human beings use to recognize other people and then see that they knew them. This is the same way the biometric software will work. The facial recognition software collects data from a face, this includes the geometry of a face, like the distance between your eyes, your forehead and chin, and as time goes so and the face grows so the scan needs to be renewed to collect the new data to have a safer authentication.

Some of the top facial recognition technologies are put out by Google, Apple, Facebook, Amazon and Microsoft. Google has put out the facial recognition software called FaceNet which has shown to have a 99.63% accuracy. Google’s software incorporates an artificial neural network to map out a more accurate facial map. Facebook also put out their own software called DeepFace program which is more simpler than FaceNet with a 97.25% accuracy.

Amazon has also put out their facial recognition software called Rekognition which is cloud-based. But this software has its controverses because not only did they partner up with law enforcement agencies. But was later reported that this technology falsely identified 28 US Congress members as people arrested for crimes.

As facial recognition software becomes more developed security has become a major topic, more specifically law enforcement. The law enforcement uses a detailed software called Automated Biometric Identification System which takes multiple types of biometric data and compare them. Using this software can help in many ways which includes finding missing children and disoriented people, find exploited children, track criminals, and accelerate investigations.

Facial recognition software has grown a lot, especially with authentication in your mobile phones, tablets and computers. Apple can be considered one of the biggest developers of this field.

The use of biometrics will only grow as technology develops. This also brings up the question of security because as technology ends up being used in very important parts of a person’s life the use of biometric authentication is one of the more secure forms of security. Since unlike the traditional passcode, the biometric authentication cannot be hacked and only be accessed through the person who set up the biometric security and has their data to match the data stored. I also see that more types of biometric authentication like the iris scan, voice recognition, palm print and many other types which are not used commercially, can be compressed and usable like the fingerprint and facial recognition because they are more reliable and when has is it ever been bad to have more ways of authentication.

Cloud Security

To talk about cloud security first we need to talk about Inhouse vs cloud storage. More and more technological and data-based companies like Well Fargo move their data which is stored “inhouse” to third-party cloud centers because to create and maintain cloud storage centers you would need very large sums of money to just maintain it. Inhouse database is defined as a collection of information related to the organization that stores internally in database. While cloud data storage is a cloud computing system that stores data through the internet, being managed by the providers as a service. Cloud can be basically defined as the ability to have data to be accessed anywhere and anytime.

Some of the most popular cloud storage providers are Apple, Amazon, Dropbox, and Google. There are many pros regarding cloud like no onsite hardware to store data. Backup and restoration of data can be triggered from offsite. Lastly can minimize data loss due to the automated regular backup of the cloud storage. While there are just as much cons with cloud storage, as I mentioned before the costs for cloud storages are exponential. There is a limit to the amount of data that can be stored due to the size and cost. Another major problem this that unlike the inhouse database this solely relies on the internet, and if the internet goes out on the providers’ side there is no chance to access the data saved.

Just stating the cons of cloud storage does not define the risks in place with using this medium. These risks include risks of cloud-based infrastructure, human error and external error. I have briefly covered the risks of cloud storage which includes the internet going down. So, we need to cover human error, Egress' Insider Data Breach Survey in 2021, has shown that 84 percent of the time services experience security problems is caused by human mistake, 74 percent have been due to employees breaking security rules in place. This is the majority of the total risk in using the cloud. While external threats are a different matter in itself.

External threats can cover many things this includes phishing, malware, ransomware, data breaches, compromised passwords and many more, all of these threats are covered in class. This isn’t really that much different with cloud storage. The cloud as I have stated above is basically data stored on the internet, thus able to access the data anytime from anywhere. This is great! Very convenient and helpful but just like with everything else the more it is convenient the higher the security risks.

For typical cyber security there are set boundaries which can help setup perimeters around it and restrict the in and out access, but how would you put a perimeter around something that has no boundaries. One of the many problems is that the cloud is so complex and vast that the IT department has no way in enforcing it thus leaving many loopholes that malicious personalities can take advantage.

Another risk is the vast connections. A malicious person can gain access to people’s information that can lead them to gain access to the person’s cloud and everything stored in it, from their personal data to important data from their workplace.

This led to many legislative actions being passed, one of such acts is CCPA. The CCPA is the California Consumer Privacy Act passed in 2018. The basic outline of this legislative act is to give users more control over the personal information that the companies collect. This law comprises of the right to know, the right to delete, the right to opt-out, the right to non-discrimination. I have discussed this act in article reviews in the past and often mention that this is only for California residents which is absolutely insane that this is not implemented throughout the country because almost everyone uses some form of the cloud.

There have been many data breaches in the recent times. The most recent data breach was the T-Mobile data breach in August 2021. The outline of this data breach was that a malicious person breached the T-Mobile servers on March 18 of the same year. This goes back to my point of the cloud being too vast that people cannot monitor the whole cloud, it took 6 months to have seen a data breach. Where this hacker stole data from not only the company itself but from the consumers as well. The data stolen includes names, drivers’ licenses, government identification numbers, Social Security numbers, date of birth and more! All these information is just what a bad person needs steal people’s identity this shows just how important security with the cloud is. Although T-Mobile put out a statement that “To be clear, we have no information that indicates any passwords, postpaid PIN numbers, or financial or payment information have been compromised.” This company took 6 whole months just to identify a breach how does this statement have any validity so it is better to always be prepared for the worst.

I have repeatedly stated this with the midterm, the article reviews and in person that when a high schooler gets their common education which includes sex-ed, English, Mathematics. The educational board should include a course in computer science, more specifically computer security, as we use computer technology will need to have the basic knowledge of what this is and how to protect ourselves from malicious people on the web.

Computer Security in the News

New-Gen robotics from Diligent Robotics shows a recent spike in casualties.

United States, 12/14/2031

Since the release of the Gen-1 home robot by Diligent Robotics in 2028, their products have seen an exponential sale. Soon after the success and the trust Diligent Robotics gained from the customers it soon began release the Gen-2 life robot and the Gen-2 multi-use robot in early 2031. 3 months into the release of the Gen-1 model Diligent Robotics discovered a data breach, but the damage was minimal due to the limitations of this model. All this model did was take care of the elderly and basically replaced an elder care specialist. All this model had was robotic arms and motorized wheels with no cameras and only sensors to increase efficiency. Diligent Robotics did not reveal this data breach and did little attempts to fix the breach due to their focus on the Gen-2 series.

Gen-2 series is a newborn baby monitoring specialist robot that takes care and monitors a newborn babies till the baby turns to 1 year old. As you guys recall the data breach occurred with the Gen-1 robot, that breach was seen in the Gen-2 robot as well.

This breach led to other major vulnerabilities that led to have compromised systems in the robot. Mountain Tech. a computer security company found this breach of the Gen-2 robot that could potentially have caused serious damage to babies, even cause death. Thank God this was sorted out soon before there were any casualties. Same cannot be said to the previously mentioned Gen-1 robot.

The Gen-1 robot soon led to many casualties with the elderly earlier this year. Edison Smith a 89 years old man who solely relied on the Gen-1 robot to live his life. January of this year there was a ransom ware attack on these devices, but due to the lack of management from Diligent Robotics the first wave of this attack led Mr. Smith to being administered the wrong medication which led to him going under cardiac arrest. Thankful the paramedics arrived on time thanks to the new gen of the flying Tesla model ambulance, this was one of the many such incidents that happened all over the country.

Due to the overwhelming pressure Diligent Robotics were forced to safely and securely shut down the systems to avoid any more casualties.

This shows that to always keep in mind as much as it is comfortable and convenient so are the risks. Since then, Diligent Robotics have been sued and under heavy fire and soon went bankrupt.

Works Cited

Biometrics Solutions. “Fingerprint Recognition.” *Biometrics Solutions |*, 17 June 2021, <https://www.biometric-solutions.com/fingerprint-recognition.html#top_ankor>.

Bonta, Rob. “California Consumer Privacy Act (CCPA).” *State of California - Department of Justice - Office of the Attorney General*, 14 July 2021, <https://oag.ca.gov/privacy/ccpa>

“Continuity Central.” *Continuity Central*, 15 July 2021, <https://www.continuitycentral.com/index.php/news/technology/6456-insider-cyber-incidents-human-error-is-the-top-cause-of-serious-data-breaches>.

“Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News).” *Thales Group*, 24 June 2021, <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition>“

The Pros and Cons of Cloud vs in House Servers.” *SysGen*, 23 Nov. 2020, <https://sysgen.ca/cloud-vs-in-house-servers/>.

Miller, William. “Different Types of Biometrics.” *Software Testing and Quality Assurance by IBeta*, 9 Sept. 2019, <https://www.ibeta.com/different-types-of-biometrics>

“Our Response to the Data Breach (Aug 2021): T-Mobile.” T, Aug. 2021, <https://www.t-mobile.com/brand/data-breach-2021>.

“What Is Cloud Security?” *Usa.kaspersky.com*, 1 Mar. 2021, <https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security>.