Biometric security now and in the future

Justice E. Thurman

04/2/2016

East Carolina University

Biometric technology has become the newest thing to implement in mobile devices, office building and is even being used to keep track of employees start and end time for work through a finger print clock out system. Biometric has come a long way since its first uses as just a filing system for criminals. With the rise of more and more private date like bank account information being stored on servers and even peoples mobile devices the need for something more secure than just a password is more prevalent than ever. The easiest thing to fill that gap is the uses of something that people with no technological background can easily use with little to no training. A finger print, iris, and a user's face can easily be used as a form of authentication. Without having to remember any long numbers or short phrases to use as complicated passwords for important information and accounts. Biometrics is being used though out the technological world and this will increase as technology becomes more integrated in to our everyday lives.

Biometrics systems used by people today can be easiest seen is in cell phones. The apple 5s brought the use of biometrics into the foreground. It used the capacitive mothed in order to capture and authenticate the fingerprint. The capacitive mothed is when the device uses the ridges of the finger to complete a circuit on the finger print reader and then render and image from that information. With the popularity of this with the public it enabled apps like Bank of Americas mobile banking app to support fingerprint authentication. Other companies like Samsung and windows also began to implement fingerprint readers in to their phones designs. Whiles the use of a fingerprint as a password with a mobile devices is very useful and much quicker than the use of a long password it also raises some important security questions. The biggest one being is the phone storing an image of the fingerprint on its hard drive and if so is it encrypted. In the case of the IPhone 5s it does indeed store what apple calls "fingerprint data"

(Tarantola). According to apple the IPhone stores this data in an “enclave of the phones A7 processor” were it cannot be accessed by any other application on the phone or by the user (Tarantola). This is one for the draw back from using biometric date on mobile devices, somewhere the finger print has to be stored. Either on the device or on the cloud were the device can connect and then compare the fingerprint. The main issues that comes with storing this data is that if it were to be stolen the consequences for the user could be dyer. With the implementations of fingerprint scanners with personal computers, ATM’s, and mobile banking apps a stolen digital copy of a user’s fingerprint allows the thief to do more than just access your phone. Also with all mobile devices that have implemented fingerprint authentications most have the user make a backup password that on some phones only has to be 4 digits long. Making the phone just at vulnerable to a security breach as it was before the implementation of a biometric password.

In today’s highly technological world more than just mobile phone are secured by biometric date. Biometric data especially fingerprints are being used in order to increase access control security. Corporations have the most of their employees only allowed in certain areas of their facilities. Even more so if the corporation manufacture something that is copyrighted or a trade secret. Therefore the use of access control security to certain part of a facilities is very important. This is even more important if the corporations houses their own data or their own servers. Companies have slowly began to use biometric data as the employees key to certain areas of a facility if they have the write clearance. One company that makes access control biometric devices is ZKTeo. They have created biometric reading devices that can be implemented any were they are need by a customer. The company also offers the use of their own software and control panels that can be implemented it to the customer’s network. Their software allows the user to not only use the system as an access control method but also be used as a time and attendance device for workers (ZKTeco). As a time attendance device it allows the manager to tell how long the person was actually at work without having to worry about another employee punching in a friend. The software allows a manager to access all the information inputted in to the device thought out the day so that while they keep out unwanted persons. This allows for the company to keep track of every employee that is in the building or even specific rooms with in there facility. This allows for more than just access control but for an ability to keep an eye on any employees without the use of a video surveillance system. If something were to be stolen from a secure part of a company's building or an unidentified person was where they were not supposed to be the manager would have the log of every person that had enter that room. Enabling him to track down the possible stolen fingerprint used or employee that let someone in. Unlike using an RFID card or CAC card biometric data cannot be stolen without access to the network or a person's fingerprint.

The company ZKTeco makes device that are more than just fingerprint some of their more high-end device can do more ant just one form of biometric identification including RFID and pin numbers. One of their most advanced biometric readers is the MultiBio 800-H. This device supports authentication through the use of face recognition, fingerprint, RFID, and numeric passwords (ZKTeco). One of the two cameras used for face recognition is an inferred camera allowing for it to detect a face even in dark environments (ZKTeco). Because of the devices multiple modes of authentication the customer can almost guaranty that no unauthorized personal will gain access. The device comes with all cables needed for implementation as well as any tools that maybe needed. The device can also be connection the customer network though a TCP/IP connection as well as having a auxiliary input allowing for a connection to alarm systems, exit buttons and smoke detectors(ZKTeco).

There are two stages to biometric security systems. The first is called the enrollment stage were the fingerprint or iris is first sampled and then stored on the device or the database. The second stage is called the release stage, this is when the biometric data is sampled again and compared to the data that was stored in the first stage to authenticate the user's identity. (L. Lai) Even with the resent strides in biometric technology there are still many different security concerns. There are two main concerns when it comes to these security issues, noise and the storage of the biometric data. Noise is the term used when revering to possible errors that can occur during measurement or errors in the data itself. "Two different measurements of the same biometric characteristics will not produce the same result, due to measurement noise or other factors such as injuries (L. Lai)". The best way to combat this frost issue is with helper data. The helper data is created in the first stage and stored on the database with the biometric information. Therefore during the second stage the system will combine the biometric measurements with the helper data to aid in finding the key. The second major concern is where and how the biometric data is stored. In order for a device to use a finger print or other biometric data to authenticate, the data in one form or another has to be stored either on the device directly or in some sort of cloud service. Both of these create a security issue and risk of thief. This is a bigger issue with biometric data than with other forms of authentication. Passwords and RFID cards can be changed and replaced while biometric data cannot. When fingerprints or faces are stored most are in a templet form. The templet security is based on the changing of the biometric date in to a security key (B. Ma). However this can cause a problem is a hacker were to find out what algorithms were used when transforming the date in to a security key. If a hacker were to gain that information and gain access to the system then not only could they have access to all the biometric data but be able to inject their own biometric data into the system. This would then make all of a company's biometric bases access control obsolete. Some forms of biometric data cannot even be transformed in to a secret keys for example face images on smart phones (B. Ma). Multiple researchers are in development of digitally water making biometric data to secure images like those used by facial recognition software.

Biometric authentication will continue to become more and more prevalent in our daily lives. As the basic items around us start to become more connected to each other and the internet so will we to them. This can best be seen through the lens of smart homes. The idea of all devices in a home being connected is great but you need to be able to secure all these devices all the way down to the refrigerator. The most basic way to secure device is with a password. However, it is not practical to use a password every time to sign in to devices with in a smart home because of how easy it is to break most passwords. Using biometric data is easy and in most cases it is secure depending on how the data is stored. One example of biometric data implemented in to a smart home is with a device called Welcome developed by CES (Biometric Trends). This device uses facial recognition software to recognize family members it can be configured to give notification for unknown faces as well as who came in what door (Biometric Trends). With the use of a device like this a smart home and its connected devices can be tailored to each individual family member though use of it just see their face. The TV could switch to their favorite channels, of it could lock certain doors if a child were in the house for too long without it seeing an adult for a pre-established amount of time. With biometric as the basis for a smart home every device or even room could be tailored to each residents needs depending on who walks in to it and is seen. As well as securing the house using a person’s fingerprint to open the door.

Biometric authentication is the way of the future because of it convenience and the uniqueness of each individuals own biometric data. It does not rely on the user’s memory of a good password or their ability to come up with a strong one. Biometric storage and a devices ability to measure the data still has a long way to go but with the use of we can simplify and steam line the authentication process. Its current uses in the fields of access control, mobile device security, and its resent expansions in to banking push the bounders of its uses. As biometric data becomes used more and becomes stored on more devices and more data bases the security of templets and other methods will have to be developed. The use of digital water-marking and the use of helper data will have to be used much more the more biometric security is implemented.

Work Cited

Aravind G, Andan H M, T. Singh and G. Joseph, "Development of biometric security system using CBIR and EER," *Communications and Signal Processing (ICCSP), 2015 International Conference on*, Melmaruvathur, 2015, pp. 0884-0888.
doi: 10.1109/ICCSP.2015.7322622 *
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7322622&isnumber=7322423

"Biometric Trends for the Smart Home." SiliconANGLE. SiliconANGLE, n.d. Web. 09 Apr. 2016. http://siliconangle.com/blog/2015/02/13/biometric-trends-for-the-smart-home

B. Ma, C. Li, Y. Wang, Z. Zhang and D. Huang, "Enhancing biometric security with wavelet quantization watermarking based two-stage multimodal authentication," *Pattern Recognition (ICPR), 2012 21st International Conference on*, Tsukuba, 2012, pp. 2416-2419. *

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6460654&isnumber=6460043

"How the IPhone 5S Fingerprint Scanner Works-And What It Means For You." *Gizmodo*. N.p., n.d. Web. 30 Mar. 2016.

http://gizmodo.com/how-the-iphone-5ss-fingerprint-scanner-works-and-what-1265703794

L. Lai, S. W. Ho and H. V. Poor, "Privacy-security tradeoffs in reusable biometric security systems," Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, Dallas, TX, 2010, pp. 1722-1725. doi: 10.1109/ICASSP.2010.5495470 * http://ieeexplore.ieee.org/sta mp/stamp.jsp?tp=&arnumber=5495 470&isnumber=5494886

Tarantola, Andrew. "How the IPhone 5S Fingerprint Scanner Works-And What It Means For You." Gizmodo. Gizmodo, 10 Sept. 2013. Web. 09 Apr. 2016.

http://gizmodo.com/how-the-iphone-5ss-fingerprint-scanner-works-and-what-1265703794

Zkteco." Fingerprint | Biometrics| Fingerprint Sensor| Biometric Recognition| Security: Zkteco. ZKTeco, n.d. Web. 07 Apr. 2016.

http://www.zkteco.com