Biometrics in Computer Security

Romaine Halstead

1204634

University of Technology

Submitted to: Mr. Ryan Meeks

Introduction

Biometric systems are coming of age, and despite all the accuracy and security concerns, it is gaining in popularity (Bleicher). With the increased reliance on technology in the lives of individuals and in the growth of businesses, there is a greater need for computer and information security. Data breaches and credit card fraud totaled 1,540 worldwide in 2014 -- up 46 percent from the year before -- and led to the compromise of more than one billion data records (Holmes, 2015). Every year hackers introduce new ways and means to breach computer security. from snooping, spoofing and phishing to social engineering, there need to be ways and measures which counteract these security vulnerabilities. Cryptography is a major field in computer science and security where data can be translated into a format unrecognizable or unreadable by third parties. It is mostly used in secure connections when transmitting data over the internet or a smaller scaled network. Cryptography is essential in mobile computing and the internet of things due to the means at which they communicate. Another field in computer science is biometric security and authentication. A proper means of authentication ensures data integrity eg. in the healthcare sector. The focus of this research paper is to discuss biometrics in computer security, its relevance in the future and the benefits it can have in the country of Jamaica.

Biometrics in Computer Security

Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics (Rouse, 2013). Biometric technology and security is mainly focused on the validation and authentication of individuals under surveillance as well as for the control of individual’s access to information and controls. The determinative factor for biometric security is the assumption that every single individual is different in their physical and behavioral characteristics. Physical characteristics may include palm prints, fingerprints, face and retina features while behavioral includes voice recondition and keystroke rhythm.

Biometric security has come a long way from being the well-established protocol it is right now. It can be argued that the use of an individual’s physical characteristics to show uniqueness traced back as far as 14th century China. Some researchers believe however that is was used mainly as a signature and that the most credible evidence of the first use of biometrics is from Alphonse Bertillon. Alphonse Bertillon was a French forensic documentarian who developed or improved upon several methods of identifying criminals and solving crimes (Cellania, 2015). Bertillon is widely known for being the inventor of the mug shot and other criminal investigative techniques. Bertillons system of anthropometry required numerous and precise measurements of the bony parts of a human’s anatomy for identification. It also involved recording shapes and size of the body in relation to movements and differential markings on the surface of the body such as scars, birth marks, tattoos, etc. (History of Biometrics, n.d.). While he never fully discovered the fingerprint, his research and inventions led to it. In the 1800s during the industrial revolution, there was need for the identification of people due to the booming population growth in cities. William Herschel in the 1870s, recognized the unique qualities offered by fingerprints in colonial India. Dr. Henry Faulds noticed fingerprints on antient Japanese pottery. He published the idea of the possible use of fingerprints in criminal investigation in a book called *Nature* which was published in 1880. Sir Francis Galton is also heavily credited in the advancement of fingerprint identification. Based on Dr Faulds research, he could conclude that every individuals fingerprint is unique and that an individual’s fingerprint will usually remain intact throughout their lives. After the second world war and the dawn of the information age, technology was advanced enough to recognize voices and read facial and iris patterns.

Currently, biometric technology has matured to a point where it is inexpensive to implement and as such, making it integrated into our everyday lives. In border security, particularly in the United States, there is wide biometric data collection at border stops and airports. Fingerprint scanning is usually done at immigration offices and iris scans are done at airports for refugees and asylum seekers. Fingerprint scanning is used a lot in criminal investigation as stated before, to identify common offenders. Before the rise of mobile computing, biometrics in computer security was more catered to large scale enterprises. This was the case because of the high costs of implementation. Currently with the high smartphone penetration rate worldwide and the need for these mobile devices to be secure as well as biometric security implementation becoming cheaper, it has now entered the consumer market. Portable laptops are now manufactured with fingerprint sensors as well as better webcams for facial recognition. This is also true for smartphones with their front facing camera. Google implemented a software based face to unlock feature in their mobile operating system in 2011. Couple years later voice to unlock was introduced which used a specific processor in the device for voice processing as well as fingerprint scanners on both Android and iOS platforms. This adds multiple benefits to the end user as a smartphone is the ultimate device for communication, doing business, entertainment and storage. It makes conducting monetary transactions much more secure and more convenient. In detail, if someone seeks to transfer funds from an account to another, they would be required to use a password which can be cracked or lost. With the introduction of biometrics, there wouldn’t be a need to use a password. Due to the physical nature of smartphones, the only reliable means of accepting and processing behavioral biometrics is through the users voice. This is mainly used for example when the user is driving as holding the device might pose a risk to their lives. However, voice recondition isn’t implemented as a rigid security feature yet and is only implemented as a perk.

Fingerprints scanners in smartphones were introduced in 2013 with the iPhone 5S and since then there have been many more devices with this feature. Currently, these scanners are very accurate, up to a 98.6% accuracy for a single finger in under 1 second (Gibbs, 2015). This means that fingerprint authentication is much quicker and easier than entering a password. Compared to face unlock albeit it’s another biometric security, there are some benefits. If there isn’t enough light where the individual is located, then there will be problems capturing a proper image of the face for identification.

There is no question as to the speed and benefit of fingerprint authentication on smartphones although there are some technologies emerging that would be more convenient than fingerprint scanning.

Mobile computing gave way to mobile payment and banking, which gave way to the need for mobile security. It’s estimated that by 2017, there will be $60 billion in mobile payment sales (Rampton, 2016). A disadvantage of fingerprints is that it could be copied. To cater to the growth in mobile security and the downsides of fingerprints, there are a few emerging technologies that could rival fingerprint authentication. There is iris scanning that translates the physical makeup of an individual’s eyes and translates it into a mathematical algorithm. The Samsung Galaxy Note 7 is one of the first and the most popular smartphones to be released with an iris scanner. The Note 7 is fitted with an infrared front facing camera that’s used to scan the eyes of an individual. Though the use of sunglasses and contact lenses might lower the performance, it works well in darker areas. Another technique is the use of 2 security measures for authentication. This greatly increases the security and authenticity of the users of the device. A common 2 factor authentication is the use of a biometric authentication along with a password or a pin code. Another trend is the use of multispectral sensors. Currently, smartphones employ the use of capacitive fingerprint sensors. In the future, there could be the implementation of multispectral sensors which scans both the surface of the finger as well as the tissue which lies beneath the skin. This technique eliminates the possibility of fingerprint copying with hackers. Though one still needs to remove their gloves to use this feature.

Overall, there are some concerns with biometrics on a whole. As stated previously, fingerprints can be copied relatively easy. Researchers have gained access into smartphones using dental molds and playdough. You would need the actual finger to make the mold in that case. This would be one of the primitive ways to do bypass the security as researchers at CITER pull off a similar trick with a 3D-printed mold, developed from a stored image rather than a real finger (Brandom, 2016). Jan Krissler, a German hacker, used high resolution photos, including one from a government press office, to successfully recreate the fingerprints of Germany’s defence minister (Hern, 2014).

Another concern with fingerprints on smartphones is not necessarily technical but more of a legal matter. In the United States, a police officer can order you to unlock your phone with your fingerprint. Because the constitutional protection of the Fifth Amendment, which guarantees that “no person shall be compelled in any criminal case to be a witness against himself,” may not apply when it comes to biometric-based fingerprints (things that reflect who we are) as opposed to memory-based passwords and PINs (things we need to know and remember) (HOFMANN, 2013). In other words, if you are under investigation which you need to unlock your phone, A warrant can be issued for you to use your fingerprint. But in the case, you use a password, you are protected under the 5th amendment and you are not required to provide it. These laws might differ for different countries however.

Some people are reluctant to the idea of storing their fingerprint or iris data on their devices, fearing that hackers would gain access to this data. This claim is justified, as there are numerous ways that a hacker can collect fingerprint data from a smartphone. An attacker could create a specially crafted app that mimicked the phones unlock screen. When the victim swipes a finger to unlock the phone, they're using their fingerprint to seal a financial transaction (EDDY, 2015). In some smartphone manufactures devices, the fingerprint sensor isn’t fully locked down, meaning attackers can gain access to the users fingerprint directly. This technique allows hackers to harvest fingerprint data on a large scale (Whittaker, 2015). This is very dangerous and smartphone OEMs should be required to ensure the data from the sensor is encrypted. This is necessary as the use of information technology and smartphones increases in developing countries, more specifically with the island of Jamaica.

Biometrics and Smartphones in Jamaica

In Jamaica, people often have the saying, If America sneezes, Jamaica catches a cold, meaning trends and startups beginning in the United States are fully matured by the time they are introduced in Jamaica. This is usually caused by the different laws and regulations between Jamaica and the United States, as well as economic factors- United States is an industrialized country and Jamaica is a developing country. While the saying is true in some aspects, it does not apply to the smartphone industry right now. After Research in Motion suffered heavy losses and had to decrease smartphone manufacturing, as well as the introduction of more budget oriented devices, Jamaica became a thriving market with the two major carriers’ providing the top of the line phones.

A report conducted in 2015 by the Office of Utilities Regulation, Jamaica’s communications and utility regulatory agency, states that internet penetration rates are at 5.4%. The then Technology Minister Phillip Paulwell disagreed stating that this figure didn’t take into account the smartphone data subscribers which would push the percentage up to 40%. The report also stated that smartphone and traditional mobile phone penetration was at 105% (Thompson, 2015). Digicel, Jamaica’s leading mobile carrier stated that over a million of its subscribers used smartphones, about 45% of its users (Digicel Jamaica's smartphone users surpass 1 million, 2015). These statistics shows how much smartphones are involved in and changing the way of live of Jamaicans. The same factors that drive smartphone growth around the world are just as much the same in Jamaica. Individuals use it for communication mainly across the internet and social media. Facebook, Twitter, Instagram and WhatsApp are dominant forces within the industry while traditional mobile network calls and short messaging system texts are being phased out. Entertainment is also a big factor. The internet, being the platform for music and other forms of entertainment and smartphones allowing easier access to it, makes it another driving force which competes against radio and television outlets. Music streaming is an emerging trend in Jamaica where subscribers pay a monthly fee for music. Online transactions and mobile banking is the third factor in the Jamaican smartphone industry. Though this concept is relatively new, banks are investing heavily in the idea of mobile banking. The National Commercial Bank, the leading commercial bank on the island, implemented a mobile money transfer system called Quisk. Quisk is a secure, mobile money account that will enable people to send and receive money and pay via text messaging (BENNETT, 2016). NCB highlighted the benefits of this system to users, citing the reduced costs associated with transporting and securing cash to other Quisk users. Conec is another mobile payment option. It started out as a gateway to pay bills and top up pre-paid mobile accounts. Currently the mobile wallet service allows merchant services and person to person transactions (COLLINDER, 2016). Along with mobile wallet solutions emerging in the country, other banks are beginning to implement smartphone applications to effectively facilitate mobile and internet banking among its customers. Sagicor, JMMB, ScotiaBank and NCB all have online banking solutions. Scotiabank and Sagicor have smartphone applications which allows users to bank online through their smart devices. The managing of accounts, transfer of funds, payments of bills and viewing bank statements are much more convenient to end users as well as making these business processes cheaper. Traditionally, account management and funds transfers would require customers to physically walk into the branch and speak face to face with employees. These processes cost time and human resources which then, in turn cost the business money. With Jamaican businesses and citizens relying so much on mobile computing, all this flow of information needs to be protected.

There are many occurrences that justifies the need for proper computer security. The internet is known for making the world smaller, drawing people closer together, whether they are good or bad. Your device being on the internet makes it vulnerable to attack on almost anywhere on the planet, that is, if you don’t have a secure device. In 2009, the then prime minister Bruce Golding fell a victim of credit card theft. Golding told fellow parliamentarians he had the shock of his life after his bank told him that thousands of US dollars in purchases were made on his Jamaican-issued credit-card account during a two-day spending spree (Hamilton, 2010). These transactions were made to purchase plane tickets in the United Kingdom. This shows the stretch and the reach of these hackers, to remotely acquire the credit card information of the prime minister of Jamaica. Minister Golding stated that tackling cybercrime is particularly complex because it allows for virtual anonymity. "It is what they call illusive scene of crime," he pointed out. One of the ways hackers capture credit card information is through email phishing where individuals are fooled into providing info to a website that was linked in an email. This vulnerability is very common worldwide and is affecting more and more Jamaicans every year. The Bank of Jamaica, The Jamaica Constabulary Force and most of the major banks issued statements to their internal and external clients about fraudulent emails being sent around.

While the possibility is there to steal credit cards remotely, local based hackers are finding their own way to capture individuals’ payment information. It has been discovered that criminals tamper with automated teller machines using hardware devices to capture PIN numbers and credit card data in the a few parishes (Fitz-Henley, 2015). Though this ATM tampering was only done in a couple of parishes, within a 72-hour period customers were robbed over a million dollars out of their accounts. Proper authentication of individuals when making transactions would potentially put a stop to these unwarranted actions.

The use of biometrics isn’t as common in Jamaica as it is in the United States. It is used in passport and immigration offices on the island, its used in the police departments and in general elections. The most prevalent option is the use of fingerprints. These techniques don’t help much in computer security as the main issues being faced in Jamaica is the lack of user authentications. The best option is with the use of smartphones to prove that the user has authentication to conduct transactions and to confirm and approve such transactions. Smartphones with fingerprint sensors are getting cheaper and more budget oriented, which means this technology is more readably available to use. In the case of Minister Golding, a system could have been in place where he would confirm the purchases from his account of which he would reject. Afterwards how would have notified his bank about his credit card being compromised. Though this happened in 2009, the technology is here now to prevent a hacker from stealing money using the prime minister’s credit card information. With mobile money trending in Jamaica, fingerprint sensors can further improve the security of these transactions. It could essentially authenticate both the sender and the receiver, giving confidence to both parties that their identities are confirmed. This is also true in mobile banking, where there is the need for authentication the fingerprint sensor would be used to login and confirm payments. Having this system in place would potentially lower the chances of being compromised.

The cost to implement these systems are quite inexpensive being that the actual technology would be a feature of the smartphone being used by an individual. There is only need for small changes in the mobile applications for them to accept fingerprint confirmation. An example is with PayPal, an online wallet and payment system. Fingerprints can be used to log into a PayPal account to enhance security. The local banks could follow suite.

However, the main question is whether it is a viable option in Jamaica. It is a good security feature once implemented correctly but it relies too heavily on the need for customers to have the sensor on their devices. Budget devices with fingerprint sensors are emerging, but they are not yet at a position in the market for this fingerprint system to be effective as it will only cater to the needs of a few individuals with sensors on their devices. Once the market is mature enough, that is, when there are many devices with sensors, then the viability of fingerprint authentication is increased.

The banking sector is not necessarily the only potential beneficiary of fingerprint authentication. Government to citizen services could get a huge impact with this technology. The Electoral Office of Jamaica use fingerprint sensors in general elections to identify citizens who would like to cast a ballot. Theoretically the use of sensors on smartphones could reduce the costs of the electoral process by having persons cast their ballot on their smart device. This is one of many uses of fingerprint authentication that the government could consider.

Jamaica is growing rapidly; its people are adapting quickly to newer technology and our culture is evolving. If implementation of this system requires more smart devices with fingerprint sensors we need not wait too long.

# Works Cited

BENNETT, K. (2016, August 19). *NCB launches into mobile money*. Retrieved from Jamaica Observer: http://www.jamaicaobserver.com/business/NCB-launches-into-mobile-money-\_71148

Bleicher, P. (n.d.). Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity. *Applied Clinical Trials*. Retrieved 2 18, 2017

Brandom, R. (2016, May 2). *Your phone’s biggest vulnerability is your fingerprint*. Retrieved from The Verge: http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

Cellania, M. (2015). *Alphonse Bertillon and the Identity of Criminals*. Retrieved from Mental Floss: http://mentalfloss.com/article/59629/alphonse-bertillon-and-identity-criminals

COLLINDER, A. (2016, July 17). *BOJ issues first mobile wallet licence*. Retrieved from Jamaica Observer: http://www.jamaicaobserver.com/business/BOJ-issues-first-mobile-wallet-licence\_67229

*Digicel Jamaica's smartphone users surpass 1 million*. (2015, January 4). Retrieved from The Observer: http://www.jamaicaobserver.com/business/Digicel-Jamaica-s-smartphone-users-surpass-1-million\_18201974

EDDY, M. (2015, August 11). *Here's How Hackers Steal Fingerprints From Your Phone*. Retrieved from PC Magazine: http://www.pcmag.com/article2/0,2817,2489262,00.asp

Fitz-Henley, A. (2015, September 15). *BEWARE!! ATM SCAMMERS AT WORK!* Retrieved from Nationwide News Network: http://nationwideradiojm.com/beware-atm-scammers-at-work/

Gibbs, S. (2015, December 27). *2015: the year the fingerprint sensor stopped being a gimmick*. Retrieved from The Guardian: https://www.theguardian.com/technology/2015/dec/27/2015-fingerprint-sensor-smartphone-security-biometrics-data

Hamilton, P. (2010, February 14). *Hackers Got Golding*. Retrieved from The Gleaner: http://jamaica-gleaner.com/gleaner/20100214/lead/lead21.html

Hern, A. (2014, December 30). *Hacker fakes German minister's fingerprints using photos of her hands*. Retrieved from The Guardian: https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

*History of Biometrics*. (n.d.). Retrieved from Global Security: http://www.globalsecurity.org/security/systems/biometrics-history.htm

HOFMANN, M. (2013, December 9). *Apple’s Fingerprint ID May Mean You Can’t ‘Take the Fifth’*. Retrieved from Wired: https://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/

Holmes, T. E. (2015, september 16). *Credit card fraud and ID theft statistics*. Retrieved from nasdaq: http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388

Rampton, J. (2016, June 17). *The evolution of the mobile payment*. Retrieved from Techcrunch: https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/

Rouse, M. (2013, December 13). *Biometrics*. Retrieved from techtarget: http://searchsecurity.techtarget.com/definition/biometrics

Thompson, T. (2015, February 4). *Paulwell Not In Full Agreement With OUR Internet Penetration Report*. Retrieved from Jamaica Gleaner: http://jamaica-gleaner.com/gleaner/20150204/lead/lead2.html

Whittaker, Z. (2015, August 5). *Hackers can remotely steal fingerprints from Android phones*. Retrieved from ZD Net: http://www.zdnet.com/article/hackers-can-remotely-steal-fingerprints-from-android-phones/