UNIVERSITY OF CENTRAL FLORIDA

FRONTIERS IN INFORMATION TECHNOLOGY

COP 4910

CLASS FINAL REPORT

Abstract

This report brings together the final papers presented by the students in the Frontiers in Information Technology class, COP 4910 during the Spring-2015 semester. In addition, it is worth mentioning that this semester the students attended 76 talks and each student gave 4 presentations. In each talk they had to present the technical aspects of the selected topic along with its social impact, ethical aspects, and professional impact.

Biometric Security

John Sensback
Frontiers in Information Technology
University of Central Florida
Orlando, United States

Brian Salvo
Frontiers in Information Technology
University of Central Florida
Orlando, United States

- ***Abstract*—**Biometric systems and the technology is an ever increasing market of our everyday lives. It is used for security to prevent fraud and it aids in the apprehension of criminals, as well as many other applications. The earliest methods of biometric security included fingerprints in clay tablets and signatures on documents. Over the past two centuries, biometrics have evolved to encompass a variety of outlets to increase the value of everyday lives. Today, not only is the government using retinal scans, voice recognition software, and fingerprint recognition, but banks are using voice recognition algorithms to authenticate users and cell phones are now unlocked only with the user's fingerprint. While this technology is clearly more secure and accurate than its predecessor, it is not a perfected science and there are potentially a variety of personal and social problems. With the advancement of this technology, many ethical issues will arise. These vary from government spying to the loss of online anonymity. The science behind biometrics could potentially move us into the new age of security, but at what cost of personal privacy?

Keywords—biometric security; biometric

I. Introduction

In everyday activities, people rely on some form of security to get us through the day. Whether they are logging into our Facebook or trying to access their emails, they depend on security to ensure the safety of their data. The current way an end user can help protect their personal data is to create unique and complicated passwords. Once the passwords have been entered, the user relies on the strength of the encryption method to protect them. Security is not guaranteed, even with these complicated passwords. Ultimately, there is a better way to protect personal data. Biometrics is a way of using the one thing only an individual has access to. Themselves. Using their biometric identity to protect their data may be one of the best ways to accomplish a higher level of protection. The term biometryis known to be "derived from the Greek words "bios" (life) and "metron" (to measure) [1]". In a sense, biometric recognition is the science used to identify a person based on physical attributes

The very first form of biometric recognition starts with the earliest humans. Babies are born into this world recognizing their mother's voice. Soon after, they learn to recognize important facial features. As they develop into adults, they were able to identify family members, friends, and enemies. Even the earliest forms of art in caves left by cavemen have forms of a biometric "signature" in the form of handprints [2]. Biometric security started to show up around 500 BC when Babylonians would imprint their fingerprint into clay tablets to identify their ownership of cargo or children. It was not until the late 1800s when police departments starting using fingerprint recognition to speed the process of the identification and apprehension of suspects. Within the next century, government and security organizations are now able to use almost every part of the body as an identification method.

In section II, we present the different types of biometrics, procedures, and applications such as: Iris recognition, fingerprinting, facial recognition, and DNA analysis. In section III, we will provide technical examples in real world environments. In section IV, we will review the social impact of the growing popularity of biometrics. In section V, we will discuss the ethical issues, impacts, and disadvantages to society. In section VI, we will discuss the professional impact and career opportunities. In section VII, we will review with a conclusion.

II. Types of Biometrics

Iris recognition is often used in areas of high security and is generally regarded as the most accurate [3]. Within the iris itself are completely random patterns that are unique to the individual. The computer scans the

iris of the user and computes an algorithm that identifies these random patterns. The user is granted access when the correct patterns are confirmed.

Fingerprinting is the most commonly recognized form of biometric security. Fingerprints have long been a way for authorities to identify suspects that were potentially at a crime scene. Fingerprints are also used by consumers to access personal locks and devices. The iPhone 6 and Galaxy S5 have the option to use your fingerprint as a way of unlocking your phone.

Facial Recognition is also a new and unique way you can unlock your phone. Once set up, all you have to do it look and you screen and blink and if it matches then your phone will unlock. Facial recognition can be used in many other ways such as camera surveillance of high security areas or to auto tag users in pictures on social networks.

A person's DNA can also be analyzed for biometric identities. DNA can be found in any kind of fluid sample. Although DNA is not currently used for any kind of biometric security, it is used for crime scenes and paternity tests.

One of the newest forms of biometric security is emerging as a palm vein recognition. Fujitsu held an innovation contest to improve and facilitate the use of palm vein recognition. Similar technology has already been implemented in ATMs around the globe. Table I shows the false acceptance and rejection rates for various forms of biometrics with intentional focus on the palm vein results [4].

TABLE I.
FUJITSU'S PALMSECURE FALSE ACCEPTANCE AND REJECTION RATE COMPARISON.
AS OF 2014

False Acceptance Rate (FAR) & False Rejection Rate Comparison (FRR)

Authentication Method	FAR (%) =	If FRR (%) =
Face recognition	~ 1.3	~ 2.6
Voice pattern	~ 0.01	~ 0.3
Fingerprint	~ 0.001	~ 0.1
Finger vein	~ 0.0001	~ 0.01
Iris/Retina	~ 0.0001	~ 0.01
Fujitsu Palm vein	< 0.00008	~ 0.01

According to Table I, the procedures of Fujitsu's palm vein recognition, PalmSecure™, has the lowest levels of false acceptance and false rejection. This means that the palm vein recognition technology could perhaps be the most accurate form of biometric security.

Fujitsu also provided a chart displaying the accuracy and practicality of various forms of biometric recognition, as shown in Figure 1 [4]. This proves their claim that the palm vein recognition technology has the highest accuracy and practicality.

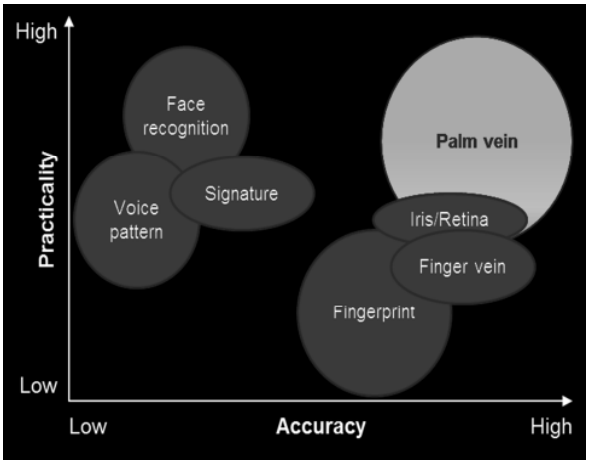

Figure 1: Fujitsu's display of an overall view of the accuracy and practicality of various types of biometric applications.

Notice how the fingerprint has high accuracy but low practicality. This is due to the requirement of the person being physically present for the scan. Whereas a facial recognition has low accuracy but high practicality because cameras around the world implement this technology to scan facial features as the person is going about their daily lives.

III. Technical Examples

Biometric Security has many practical uses in today's day and age. With the amount of cyber security attacks, people need to implement a more efficient encryption method to protect themselves and their data. Biometric security can do just that. Since everyone has a unique DNA structure, no one can have the same "password" as another, in a biometric sense. This allows for a better password system than what is available today.

Criminal identification is another useful reason to further current technology in biometrics. Officials can better protect locations of interest, such as banks and schools, if they can identify potential threats as they approach or even enter the building [5].With facial recognition, customers can be ran through a criminal

database in real time as they pass by the front door cameras.

A type of technology used every day is the ability to talk to devices. People use their voice to hands-free type, complete online searches, and do many other tasks. The advancement of technology is allowing this method to go a step further. Not only can the voice be used in a software function, it can be so ONLY a unique voice pattern belonging to the individual can complete these tasks. Nuance Communications creates technology that allows the user to use their voice to communicate with technology. They are currently creating a way to recognize patterns in the voice structure and use it as a password. Currently being on trial with banks, users can call their bank to access accounts by simply saying "my voice is my password". This eliminates someone being able to falsely access sensitive information.The largest deployment of any biometric is what makes this technology possible. Sprint's Voice FONCARD® which makes use of TI's voice-verification engine.

IV. Social Impact

Biometrics have a huge advantage to the advancement of social lives. Facial recognition can be deployed in interconnected cities to identify a missing person or potential criminals. Cases would be closed faster, freeing up time and allowing for law enforcement to focus on more immediate concerns. Fingerprinting has also worked its way into an aspect of everyday lives with cell phones now capable of fingerprint recognition. Instead of typing in a passcode or swiping in a certain pattern, a user can just simply hit the home button, which is usually always the first action performed. The fingerprint is analyzed and it is matched to the database. If the print has access to the phone, it will unlock. One of the largest entertainment mediums, video games, will have been impact by these tools as well [6].

V. Ethical Issues

With the advancement of this technology, ethical issues become a huge concern. This technology can be misused by the government or other entities for various purposes. If facial recognition technology were to be more advanced, who is to stop it from being used on every video recording device? If there is a "criminal" database with fingerprints, iris scans, and facial recognition, anybody in that database could be tracked, regardless of where they go. What if it expanded to more than just criminals? Any person of interest could be tracked anywhere in the world, in real time. This leads to the integral degradation of personal privacy.

An issue that can affect society as early as this year is the removal of online anonymity. If a user were to tie their online profiles to their physical features, would the time of the "anonymous internet"be no more? Passwords will always be an integral part of the internet, but when the majority of websites make biometrics a requirement would a user be inclined to use these biometric methods if it guaranteed data protection? These are all considerations one must make as they choose to proceed down this path as technology advances [7].

VI. Professional Impact

A. Job Opportunities

As with any technological field when the technology advances, so do the career opportunities. Any large government organization will most likely have some form of biometric security. Entities from local law enforcement to government agencies, such as the FBI and CIA, rely on biometric technology almost daily to perform tasks [8]. A career with any of these organizations will most likely merit a situation in which biometrics can be used, but these applications will only be on the end user level. A person will have to be highly technically trained in order to be part of the force that designs, creates, or implements biometrics.

B. Careers

An example of a career in biometrics would be a Biometrics Engineer. A biometric engineer is generally a software developer who creates and maintains various biometric systems [9]. A Bachelor's degree in a Computer Science or related field is a common requirement. In addition to having strong computer programming skills, a biometrics engineer will have strong problem-solving skills and an extensive comprehension of biometric systems [10]. According to SimplyHired.com, the average biometric engineer salary is $78,000. Many of these professionals hold graduate degrees, granting them more pay.

As you can see in Figure 2, the biometric industry is on a steady incline and constantly growing. This information was provided by Acuity Market Intelligence [11].

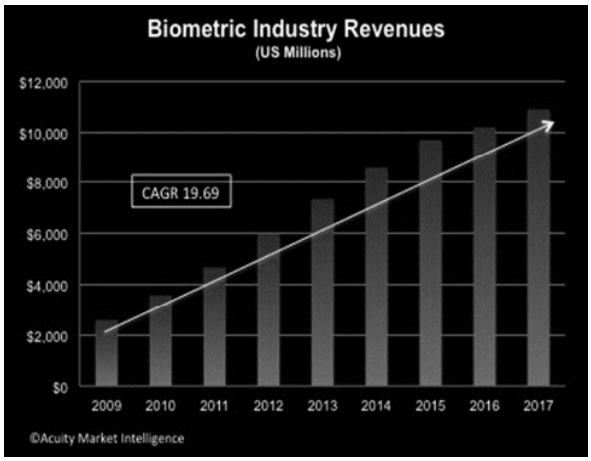

Figure 2: The Future of Biometrics; 2009 Revised Edition

VII. Conclusion

Biometrics are quickly becoming a part of everyday lives whether society wants it or not. As new technologies are developed, so will new biometric methods and algorithms. This technology can be crucial in how sensitive information is secured and how society goes about its everyday life. Biometric characteristics can be used to secure sensitive information such as fingerprint scanning on mobile payments or they can be used by governments and organizations to spy on anybody's every move. As with every advancing technology, there will be cons and pros. We, as a society and species, have to believe that the pros will always out-weigh cons.

References

N.V. Boulgouris, K. Plataniotis, and E. Tzanakou, *Biometrics: Theory, Methods, and Applications*, Hoboken, NJ: Wiley, 2009.

K. Saeed and T. Nagashima. *Biometrics and Kansei Engineering*, New York, NY: Springer, 2012.

A. Jain, R. Bolle, and S. Pankanti. *Biometrics: Personal Identification in Networked Society,* Norwell, MA: Kluwer, 1999.

FUJITSU PalmSecure Innovation Contest. (n.d.). RetrievedMarch 25, 2015 from https://www.innovation-ideacontest.com

Central European Conference on Information & Intelligent Systems. *Biometric system reliability as an important factor of influence on Chain of Custody of Digital Evidence.* Sep 2014

Information and Privacy Commissioner of Ontario. *Facial Recognition with Biometric Encryption in Match-on-Card Architecture for Gaming and Other Computer Applications,* Torronto, 2014..

Information and Privacy Commissioner of Ontario.*Privacy by Design Solutions for Biometric One-to-Many Identification Systems,* Torronto, 2014.

Biometric Technology Today. *RBS and NatWest mobile customer log in with fingerprint biometrics*. Volume 2015, Issue 3

Biometric Technology Today. *NXT-ID files patent for voice recognition-based payments.* Volume 2015, Issue 3

Biometric Technology Today. *ZTE Grand S3 to feature eye-based biometrics from EyeVerify.* Volume 2015, Issue 3

Acuity Market Research Reports. (n.d.). Retrieved March 27 2015, from http://www.acuity-mi.com/FOB_Report.php