Project plan for degree project

Version 1 – March 27, 2021

PA2554: RESEARCH METHODOLOGIES IN SOFTWARE ENGINEERING

June 3, 2021

Thesis	Tentative title	Biometric security and authentication: An Overview
	Classification	K.6.5: Security and Protection; H.1.m: Miscellaneous
Student 1	Name	Robert Mihaila
	e-Mail	romi20@student.bth.se
	Social security nr	990826T119
Student 2	Name	David Centellas López
	e-Mail	dace20@student.bth.se
	Social security nr	000505-T032
Supervisor	Name and title	Nauman Ghazi
	e-Mail	ngh@bth.se
	Department	

1 Abstract

Context:
Biometric authentication is a security verification that will consider one or more biological features to identify that the person who is logging in, is in fact the true person logging in. There are some different biological characteristics that could take place as seen in common techniques such as finger scanning, facial recognition or voice identification.

Contribution:
This paper provides an approach to an unsure future as biometric authentication is and what security measures could be assessed.

Method:
The primary research method used is case study research. Basing our data collection on articles and documentation.

Keywords:
Biometrics; Authentication; Security; Login systems; Fingerprints; Image processing; Identification; Attacks; Password; False Rejection Rate; False Acceptance Rate.

2 Introduction

Biometrics refers to the automated or semi-automated recognition of individuals based on their physical, behavioral or psychophysiological traits. These traits include face, fingerprints, iris (physical); gait, keyboard typing pattern, signature (behavioral); and saccadic eye movement (psychophysiological). Belonging to one type of authentication, based on what we are, it is not to be forgotten the other two rather common types. Based on what we know, as passwords or PIN, and based on what we have, as a USB containing the key.

Authentication using biometrics is considered to be an easy and unique method for all people to log into their own accounts, regardless of the organization working in. This is an urgent matter to develop as security takes time to be implemented and deployed. While passwords are in used in the majority of occasions, some tending to be as easy as “password” or “123456789”, biometrics ensure a unique and “nontransferable” method for authentication. An improvement on biometrics authentication could change the world, at least in security implementations. The use of biometric authorization has levelled up as a single authentication factor especially in the enterprise sector [4], reaching to valuable research literature enhancing security, with special attention towards two specific rates that ought to be considered, False Rejection Rate and Fake Acceptance Rate. This rates happen to be what is known as false negative and false positive approaches to biometric authentication.

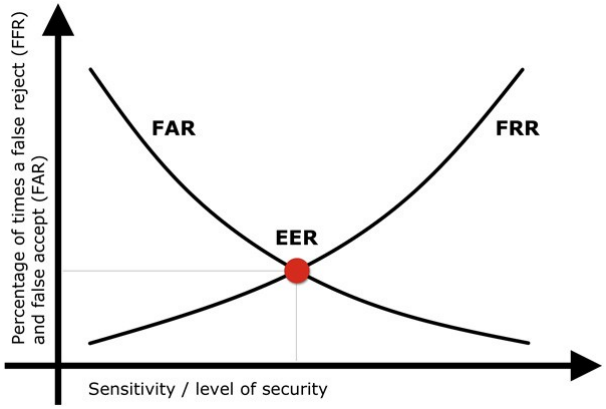

Figure 1: FAR-FRR

The aim of this paper is addressing security for biometrics authentication, concluding in some ideas or solutions to be discussed. This research is taking into consideration aspects from the “new technologies”, such as IA [2] and how could that trick biometrics authentication. Its implications will have a repercussion on the society itself, awarding population with a safer way of identification over passwords for each different service. In other words, a safe biometric authentication system should be able to ensure the user´s personal data, making it impossible to be accessed by any other user, even in the same device unless needed.

This paper will address biometric authentication from different points of view, ranging from its problems towards its solution getting through different unsuccessful mechanisms that could be easily exploited in the "wild". In order to place the problem into context, it is to be considered the increasingly number of options that are combining biometrics and authentication methods nowadays [5]. Special inquiry will be made around Jan Krissler work [6] [7].

3 Related work

Different literature regarding biometrics is being continuously developed as its uses are growing exponentially, but not always successfully. It is not needed to go back a lot of years in time to see the first remarkable "failed" approach towards the use of biometrics in commercial phones as it could be seen in the following newspaper headline dated to 2014:

Hacker fakes German minister's fingerprints using photos of her hands.[7]

Jan Krissler, also known as Starbug, is the actor behind this threat. He is a German hacker and computer scientist better known for his work on bypassing or deceiving TouchId feature on IPhone. However, one of his latest papers [1], has started the discussion of a three-step authentication method, degrading the aspect of biometrics to something publicly known that will work as a unique identifier. It has a clear motivation, improving the security quality by adding an extra layer for identity management. It reduces the risk for different threatening attacks that are to be determined in these evolving technologies as its complete authorization is not based on an only factor authentication.

Another use undergoing investigation is its suitability as a method of authentication for payment purposes, which is rekindling the idea for a card-less society [6]. As stated, biometrics have developed from just a fingerprint to further recognition and image preprocessing in less than ten years. In this continuous evaluation of the process, two-factor authentication integrating biometrics happened to be an upgrade to the system. In order to demonstrate this fact, different research has been carried out by implementing keystroke dynamics [3]. The outcomes offer 99.5% accuracy, deriving in low false negative rates and almost negligible false positive rates.

4 Research Methodology

In this section we describe the objects, subjects, treatments and the design. The primary research method used is a case study research and we will base our data collection on articles and documentation. Then, we will make a qualitative data analysis to understand and interpret data, in order to answer the research questions below:

4.1 Research Questions

RQ1: Is biometric authentication safe?

It is a discussed matter that nothing is completely safe and everything has its own flaws. This is, what is safe now, could become deprecated or obsolete in the blink of an eye. Even more if we address the issue of the logarithmic scale all technologies are growing with. Therefore, the first questions that comes to our mind when a new authentication method is implemented are: is this new technology safe? [14] If we do this change in our company, will it be more secure? Do we have the necessary techniques to ensure the integrity of our users?

RQ2: Is it suitable nowadays to implement biometric sensor systems?

Old authentication schemes (password, pin, patterns, etc.), nowadays, are still the most common methods to validate our identity [15].Thus, changing the whole infrastructure to a completely new and different security control of access could incur a very high monetary cost. But, the system that most of the companies have already, is it free to maintain? I is the method that users prefer? What if the biometric systems are beneficial in a medium/long term?

RQ3: Do we have the technology, methods or algorithms to detect fake biometric data?

The creation of this new and complex authentication systems has led cybercriminals to try to hack it by creating fake and malicious data for nefarious purposes *[Figure 3]*. When images posted on the Web are used for determining the identity of a person, an erroneous match due to perturbations in the images can have serious consequences. Therefore, it is essential for a biometric system to validate the integrity of the input digital media prior to processing it [16].

RQ4: Is biometric authentication accepted by the users?

In terms of technology, biometric systems seems to be the future in this area of cybersecurity. But, what do people think about this new methods of authentication? [14] Do they feel more secure using their human body to log in their accounts? Do they trust it? Do they prefer this new method rather than the classic ones (passwords, pin codes, lock screen patterns, etc.)?

RQ5: Where not to use biometrics?

Although good for user authentication, biometrics can't be utilized to validate PCs or messages. Biometric qualities are definitely not secret and hence they can't be utilized to sign messages or scramble reports. On the off chance that my unique finger impression isn't secret there is no sense in adding it to reports we have composed. Any other individual could do likewise. Cryptographic keys got from biometric information are jabber, as well. Far off biometric validation isn't paltry in any way. The presumption that any individual who can give my unique finger impression can likewise utilize my bank account in the home-banking application is anything but a smart thought.

4.2 Case IPad and context

This is a real case that happened to us a few weeks ago. It is about Siri's voice recognition. When you say the words "Hey Siri", if you are the owner of the device and you have configured this functionality by doing various voice tests, it is activated and responds with a friendly "how can I help you?". We were together with two different Apple devices and both have Siri configured with the voice of their respective owners. Both devices are working correctly and there was no previous problem with voice recognition. So, when one of us said "Hey Siri" and tried to give a command to his own iPad, it did not recognize the voice and did not give any sign of life, but the other person's Mac Book began to speak and interpret the command. This was completely unexpected since the voices are very different.

4.3 Case IPad Data Collection and analysis

We have used our own example from real experience as evidence to do an analysis and answer the questions. Apple's own page offers the necessary information to get an idea of what Siri is and how it works [8]. Regarding RQ1, we can affirm that it is not safe since with this example we managed to do the Spoofing and impersonate the identity of another person. Furthermore, this is not the only vulnerability we have found. If we record the voice of the owner, we can play it and Siri will not make the difference between the original voice and the audio recorded [11]. In this specific case, Siri does not have much functionality available, and it cannot unlock the device either, so RQ3 cannot be answered concisely as there is no direct comparison with traditional authentication methods. For the RQ4 we can consider different solutions such as that Siri also requires the user's face to do a double check. But here it is again the problem we mentioned before, user comfort. If the user is in a position where the camera does not detect him, then he will not be able to use Siri either and it is a hassle to always have to be posing with the face if you want to give Siri an instruction as simple as "play music" or "raise the volume". This is something that must be taken into account since it is useless to have a very safe product if nobody uses it.

4.4 Case and context German Minister of Defence (short)

The idea behind this act is simple but hard to get away with in a context of a high-level politician or celebrity. The act itself is replicating the fingerprints of someone who is continuously appearing on the public scene, due normally to its powerful position or valuable social status. The first biometric authentication methods only used the fingerprints in order to work and successfully login into the device. This method was restored in society after Scotland Yard adapted the already known technique for criminal identification. This rudimentary method of authentication derived in fingerprinting spoofing in the digital era. It only needs image processing software and a high amount of data to be analysed in order to duplicate any possible fingerprint with a high success rate [11]. It is an attack that consists on impersonating another person identity. As a consequence, fingerprinting authentication mechanisms suffered a deep investigation that lead to considering further methods such as thermal sensors [1]. This happened to the IPhone 5S, one of the first models in the market with this mechanism [7].

4.5 German Minister of Defence Data collection and analysis(short)

The data to be retrieved from this case happened to be some high-resolution photos, some even given by her own press office [7]. These derived into a full model of the German Minister of Defence, Ursula von der Leyen, fingerprints. To perform this task, an app called 'Verifinger' was used. If we have physical access to her phone, it could have been a disaster as personal information will be released.

Not only important people were in this risk, Krissler was able to hack into the IPhone 5S fingerprint method in less than 24 hours [7]. Exposing a security threat on a large scale for people that would not be aware of the risk they were exposed to.

5 Expected outcomes

Monetary costs are a main factor to take into account as well. It is not possible to implement biometric authentication systems if we have not carefully analyzed the costs that it would entail, not only in a short period of time, but also in a medium and long term. Or, if just on the contrary, it means saving money. In order to answer RQ2 we will analyze both, the costs of maintenance password to authenticate and the implementation of facial recognition systems.

To calculate the costs of password authentication method, we use an insurance company [13]. Each month, this company's help desk fields almost 3,000 password reset calls that require IT staff to contact the employee's manager to approve the reset. This is a security measure since the organization handles personally identifiable information. In these situations, resetting the password involves three people — the employee, the employee's manager and someone from IT. The password reset process takes an average of 30 minutes, time that each of the people involved loses. And, from the point of view of the users, resetting passwords can turn into a frustrating, time-consuming experience. Regarding RQ4, this is a good point in favour of biometric authentication. Averaging the amount of money each of these employees makes an hour comes out between $12.50 and $25 for half an hour. Using those figures, password resets cost the company more than $100,000 (3,000 password resets x $12.50 x 3 = $112,500) each month in productivity.

On the other hand, A major pharmaceutical company lets some employees use Windows Hello [9] for authentication, allowing them to use biometrics instead of passwords to access Microsoft applications and hardware. But adopting this technology was not free. In general terms, and answering RQ2, biometric technologies require an annual revenue by the company that it is not available for everyone. Many of the company's computers lacked the ability to read biometrics. To remedy this, the drug maker spent nearly $2 million and purchased 25,000 USB infrared cameras that cost $76 each so its workers could use Windows Hello (25,000 x $76 = $1.9 million). Continuing with RQ2 and RQ4, often times, organizations assume that Windows Hello is free to use. In reality, it requires purchasing hardware, such as USB fingerprint readers, infrared cameras or computers that can read biometrics, and upgrading to Windows 10, which can bring additional software costs. Using these two examples as premises, in two year the costs would be similar for both technologies but, and this is the best part, the users comfort and ease of use is worth it. And once this new system has been tested, it is very difficult for the user to stop using it and resort to the previous method [14].

Elaborating a demographic analysis and studying the relationship between respondents' demographic characteristics and their answers on biometric technology and satisfaction questions (RQ4), we can conclude with the following results:

"Age was significantly related to their answers about keystroke's robustness against attacks: aged respondents (grater than 28 years old) considered that the system is less robust against attacks than youngest ones.

• *For keystroke system, education level was significantly related to the disturbed, threats to privacy, verification quickness and correct answer factors:*

• *high school graduate respondents were less disturbed than the others.*

• *none graduated respondents have expressed much more concerns about their privacy than the others.*

• *high school graduate respondents considered that the computation time during the verification phase is faster than the college graduate respondents.*

• *keystroke performance was perceived better by the high school graduate respondents than the college graduate respondents."[14]*

6 Time and activity plan

On the next structure *[Figure 2]* it is possible to see the sections addressed in each step of the process to develop this paper. For the correct exposition of the data, each section should have been reviewed by authors on each deliverable. The final deliverable itself established another reviewing opportunity and refreshment of the content published, conducting into this paper.

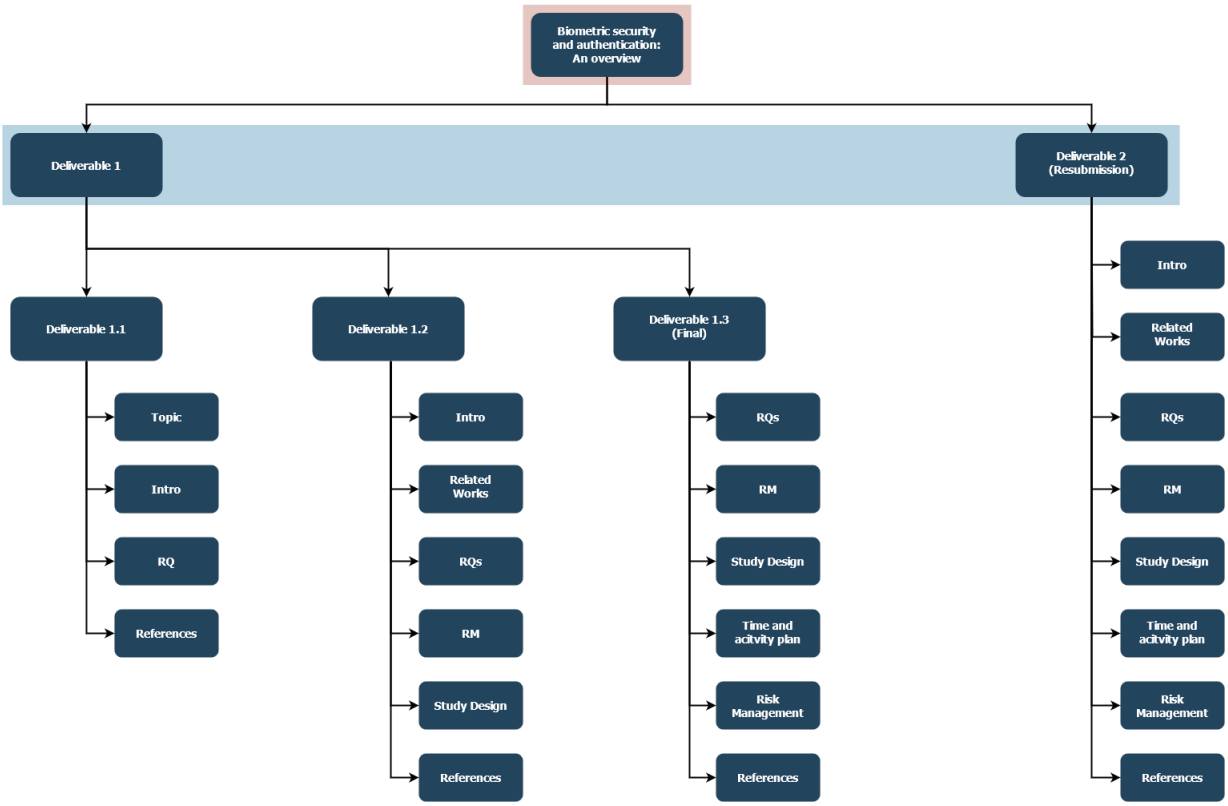

Figure 2: Work-breakdown structure

The references linked to this paper are not the only information that has been deeply investigated. Both authors have attended different lectures on deep fakes and how biometrics could be replicated or modified through different software systems leading normally to fake news. This area discovery empowered the creation and research on this topic to both find and create more literature on an evolving topic as the one it is addressed.

Towards the evolution of this paper, there has been different important risks that have been discussed and carefully mitigated. The main risks are related to the literature found and the points of view they offer. While there are studies supporting and discussing the use of three-factor authentication [1], there are others deeply encouraging its use as single-factor authentication [6]. As a consequence, there was a planned mitigation strategy taking place for the correct analysis of the data based on two factors:

• **Multiple theories:** There has been a process to contrast the information of all sources used in the undergoing investigation. The outcome offered different and plausible theories which will then be discussed in the second factor.

• **Multiple authors:** The next step on the approach is discussing the authors ideas and procedures on the analysis of the data. This ensured a wider range for points of view in the theories, which were modified, classified and finally followed in the procedure. After consensual and evidence-supported idea, the data is clearly stated and discussed during the study.

7 Risk management

Biometric authentication is an extensive field of research with different types of well-defined biometric identifiers. Focusing on the different types of biological characteristics, there are different forms of attacks [10]:

• **Attacks on face recognition:** Nowadays, face images and videos about a person are very easy to obtain. Attackers can easily get the data they want from the Internet, especially via social networks. Using those images and videos, it could be simple to cheat a face recognition system *[Figure 3]* .

Figure 3: A GAN-generated face image.

• **Attacks on iris recognition:** With the development of high-resolution camera, stealing an iris image and attack an iris-based recognition system is possible today. However, a high-end optical design always implies a high price. In other words, the cost of this kind of attacks is relatively high *[Figure 4]*.

• **Attacks on voice:** Voice is also a kind of biological signal that can be easily collected. If an attacker records user voice and replays it during user authentication, the voice-based authentication system is very likely to be deceived.

• **Attacks on electrocardiographic (ECG) signals:** Since the ECG signals must be col-

lected by corresponding electrodes or infrared sensors, this kind of attacks are easy to be detected and prevented.

• **Attacks on fingerprint and palm-print:** Many types of materials can be used to make a fake finger. Fingerprint can be collected from the surface that the users have touched, from pictures, etc. *[Figure 4]*.

• **Attacks on keystroke and touch dynamics:** It is difficult to imitate other people's behaviors. However, this kind of authentication system based on keystroke and touch dynamics is vulnerable to statistic attacks.

Figure 4: Examples of different types of spoof artifacts.
(a) Fingerprint, (b) Iris and (c) Face.

These are the most common techniques used to hack biometric systems nowadays, and cybercriminals do have really good skills executing these attack methods. But, there are several ways to prevent our identity against it. To do so, new analysis algorithms take the patterns of our hands/fingers as well as fake inputs to elaborate an arrangement to detect it in next occasions. Also, there are key generator methods [16] that would highly reduce the risk of being hacked by palm/finger printing vector.[17]. Using a two-factor-authentication based on biometrics is another recommended solution that reduces the risk probability [18]. In order to detect and prevent fake faces*[Figure 4]*, a multi-spectral analysis is an experimental and very promising technique with only 0.91 TER(Total Error Rate)[19].

As it has already been stated in this paper, in terms of security, we can never talk about an application 100% secure. In this case, the more input vectors there are, the more difficult it is to keep the percentage of safety as low as possible.

References

[1] Julian Fietkau, Starbug, and Jean-Pierre Seifert. *Swipe Your Fingerprints! How Biometric Authentication Simplifies Payment, Access and Identity Fraud.* https://www.usenix.org/system/files/conference/woot18/woot18-paper-fietkau.pdf

[2] Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. *Behavioral Biometrics for Continuous Authentication in the Internet of Things Era: An Artificial Intelligence Perspective* http://sagarsamtani.com/wp-content/uploads/2020/06/Liang-et-al-2020-Behavioral-Biometrics-An-AI-Perspective.pdf

[3] [3] Viacheslav Liskin, Egor Serdobolskiy, Iryna Sopilko, Tetiana Okhrimenko. *Two-factor User Authentication Using Biometrics* http://ceur-ws.org/Vol-2654/paper41.pdf

[4] Mohammad AlRousan and Benedetto Intrigila. *A Comparative Analysis of Biometrics Types: Literature Review* http://64.150.161.37/pdf/jcssp.2020.1778.1788.pdf

[5] Israa Majeed Alsaad. *Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review* https://www.researchgate.net/profile/Israa_Alsaadi3/publication/348662448_Study_On_Most_Popular_Behavioral_Biometrics_Advantages_Disadvantages_And_Recent_Applications_A_Review/links/6009c63b299bf14088b188e8/Study-On-Most-Popular-Behavioral-Biometrics-Advantages-Disadvantages-A.pdf

[6] S.Padma Priya. *Biometrics and Fingerprint Payment Technology* http://ijarcst.com/doc/vol5issue1/priya2.pdf

[7] Alex Hern. *Hacker fakes German minister's fingerprints using photos of her hands* https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-\fingerprints-using-photos-of-her-hands

[8] *Siri Documentation* https://www.apple.com/siri/

[9] *Windows Hello Documentation* https://support.microsoft.com/en-us/windows/sign-in-to-your-microsoft-account-with-windows-hello-or-a-secu

[10] ZHANG RUI AND ZHENG YAN. *A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8590812

[11] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A. and Minkyu Choi. *Biometric Authentication: A Review.* https://www.biometrie-online.net/images/stories/dossiers/generalites/International-Journal-of-u-and-e-Service-Science-and-Technology.pdf

[12] Sinan Kocak, Haya Altaleb, Óbudai Egyetem. *Risk of using Biometrics.* https://www.researchgate.net/publication/332079038_The_Risk_of_Using_Biometrics

[13] Veridium. *In numbers: the cost of authentication.* https://www.veridiumid.com/passwords-cost-authentication-passwordless/

[14] Mohamad El-Abed, Romain Giot, Baptiste Hemery, Christophe Rosenberger. *Evaluation of Biometric Systems : A Study of Users' Acceptance and Satisfaction.* https://hal.archives-ouvertes.fr/hal-00984024/document

[15] Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, Sarminah Samad. *Authentication systems: A literature review and classification.* https://doi.org/10.1016/j.tele.2018.03.018

[16] Joseph Mwema, Stephen Kimani, Michael Kimwele. *A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates.* https://www.academia.edu/10887642/A_Simple_Review_of_Biometric_Template_Protection_Schemes_Used_in_Preventing_Adversary_Attacks_on_Biometric_Fingerprint_Templates?auto=citations&from=cover_page

[17] Isao ECHIZEN, Tateo OGANE. *BiometricJammer: Method to Prevent Acquisition of Biometric Information by Surreptitious Photography on Fingerprints.* https://www.jstage.jst.go.jp/article/transinf/E101.D/1/E101.D_2017MUI0001/_pdf/-char/ja

[18] Andrew Teoh Beng Jin, David Ngo Chek Ling, Alwyn Goh. *Biohashing: two factor authentication featuring fingerprint data and tokenised random number.* https://doi.org/10.1016/j.patcog.2004.04.011

[19] Bensenane Hamdan, Keche Mokhtar. *The detection of spoofing by 3D mask in a 2D identity recognition system.* https://doi.org/10.1016/j.eij.2017.10.001