UNIVERSIDAD POLITÉCNICA
DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INFORMÁTICOS

MÁSTER UNIVERSITARIO EN INGENIERÍA DEL SOFTWARE –
EUROPEAN MASTER ON SOFTWARE ENGINEERING

Usability Analysis of Authentication Techniques

Master Thesis

Josué Matías García

Madrid, June 01, 2014

This thesis is submitted to the ETSI Informáticos at Universidad Politécnica de Madrid in partial fulfillment of the requirements for the degree of Master of Science on Software Engineering.

Master Thesis
Master Universitario en Ingeniería del Software – European Master on Software Engineering
Thesis Title: Usability Analysis of Authentication Techniques
Thesis no: EMSE-2014-04
June 2014

Author: Josué Matías García
Bachelors of Computer Engineering
University of Puerto Rico of Mayagüez (UPRM), Puerto Rico.

Supervisor:

Ana Ma. Moreno Sánchez-Capuchino
Full Professor

Languages, Systems and Software
Engineering Department
Facultad de Informática
Universidad Politécnica de Madrid

Co-supervisor:

Eduardo Fernández-Medina
Full Professor

Department of Information
Technologies and Systems
Escuela Superior de Informática
Universidad de Castilla-La Mancha

ETSI Informáticos
Universidad Politécnica de Madrid
Campus de Montegancedo, s/n
28660 Boadilla del Monte (Madrid)
Spain

CONTENTS

1. INTRODUCTION

Security plays an important role in today's life. Companies and individuals want their data and private information to be secure and to only be accessible to the ones that should have access to it. When dealing with security and privacy it is crucial to determine if a user is who he or she claims to be. This is where authentication comes along.

In order to deal with security, authentication is crucial. Many people have suffered from others entering into their private data, most of the times because of bad authentication processes. We use authentication not only to access our phone, but to access our email accounts, our social media, our computer, and even to transfer funds from our bank accounts. This is why authentication is such an important part of security, without it anyone would be able to access any type of data, no matter how critical or sensitive that data is.

Security in software is still an important factor in everyday life, not only for individuals, but even for big important companies. Every year we can see in the news how a big company was a victim of a hacking attack. Urging users to change their authentication methods, which for now is mostly text based passwords.

There are many authentication techniques available today. Some require a password, others require an ID card, others a fingerprint, etc. As technology advances more techniques are bound to be created in order to provide more and new options of authentication. Having an effective user authentication is critical for protecting information and system safety. Previous research suggests that some authentication methods can be hard to remember or hard to use, leaving users to use less secure but easier to use options. Various authentication applications have been proposed. However, existing research on the usability of authentication methods is limited. (Ma, Feng; 2011)

There are two main streams of research into the usability and security of various authentication solutions. Computer security research tends to focus on the ability of attackers to "crack" password solutions for authentication with little emphasis on usability. Many usability researches focus on memorability of passwords with some emphasis on user satisfaction, but with little emphasis on security implications. Another school of thought argues that poor authentication usability leads to poor security as users, as an example, write down passwords that they cannot memorize and recall. As a result, these researchers argue that it is imperative that developers design in both security and usability from the beginning of the system or product life cycle. (Tari, Ozok, Holden; 2006)

Usability has been increasingly recognized as an important factor in the acceptance of systems by end users (Cysneiros, Kushniruk; 2003). Usability evaluation plays an important role to assess the systems and user's experience (Mohd Ramli, Jaafar; 2008)

Usability can be measured through different attributes. In this thesis we will analyse how different authentication techniques behave according to specific usability attributes. This will help others who want to emphasize on a specific usability attribute for their system to

choose which authentication technique is better. In other words, this study can provide practitioners with knowledge about the impact of particular authentication techniques on specific usability attributes.

In order to address this study we will first focus on finding a classification of authentication techniques.

This document will be divided into two main parts. The first one will be the classification of the authentication techniques. We will search the main electronic databases for papers related to authentication techniques. We will then summarize the related papers and show what classifications they use for the authentication techniques. After all of the documents have been read and summarized we will analyse them and group the authentication techniques into the classifications found.

For the second part of the document we will focus on the study of usability attributes in the authentication techniques. This to know how authentications techniques compare to one another based on their usability attributes. We will search the main electronic databases for papers related to the usability attributes of authentication techniques based on the usability definition of ISO/IEC 25010 (SQuaRE) and its attributes. We will then summarize the related papers and show what authentication methods they describe and which usability attributes they measure. After all of the documents have been read and summarized we will analyse them depending on their usability attribute.

At the end we will elaborate those results to show which authentication techniques have better usability in terms of a specific usability attribute. This will help practitioners who are interested in using authentication methods but want or need to focus on a specific usability attribute. They will be able to use this as a guide to help them chose the best option that fits their purpose.

To be able to achieve these objectives the thesis will be structured in the following way:

- Chapter 2 explores the classification of authentication techniques and the process followed in order to achieve it.
- Chapter 3 explores the usability of authentication techniques based on their attributes. It shows the definition of usability and the attributes we will take in consideration. It will also show the results and the process followed in order to achieve them.
- Chapter 4 presents general conclusions to the overall topic.

2. CLASSIFICATION OF AUTHENTICATION TECHNIQUES

2.1 Introduction

In order to understand better the authentications techniques we will classify them into different types of groups.

In this chapter we first will show how our method and procedure of research will be as well as discuss the research question and how we developed our search string. We will discuss what databases we used and how many results we got. Also what our criteria was for eliminating unrelated papers.

We will then show the results and a summary of each related paper with the classification hey used. After all the papers have been summarized and analysed we will then make a discussion and will be unite them into a table of the different classifications of authentication techniques

2.2 Research Method and Procedure

This section presents the process enacted to conduct our systematic mapping study of the literature related to authentication techniques and their classification. The guidelines provided by Petersen et al. (2008) were used to build this systematic map.

2.2.1 Research Question

There are many authentication techniques used today, in order to facilitate their study we formulated the following research question:

RQ. In what classifications are the different authentication techniques divided into?

This question intends to clarify the different classifications that exist for the different authentication techniques available today. Once we have the answer to this question we will extend the mapping study to the different authentication methods and their usability.

2.2.2 Search Strategy

The search was run on several well-known databases, such as IEEE Xplore, ACM Digital Library and Inspec, as well as some individual journals and papers.
The publication year was set between 2002 and 2013 to limit the results to documents published within the last 11 years. Then, the titles and the abstracts of the identified articles

were checked against set eligibility and relevance criteria (this criterion is explained in Section 4.2.3).

2.2.3 Data Retrieval

In order to collect information that could be used to answer the research question; search strings were devised. If the database allows it the Boolean operators, AND and OR were used to do the search. The OR operator allows to include alternative words or synonyms and the AND operator allows to unite two or more words or phrases together.

X was composed of synonyms of or words possibly related to classification

X: {Classification OR taxonomy OR grouping}
Y was composed of synonyms of or words possibly related to authentication techniques, using each linked by the “OR” operator.

Y: {Authentication techniques OR authentication methods}
Finally, the “AND” operator was added between X and Y to retrieve relevant literature related to classification of authentication techniques. Search string matching was confined to terms in the title and abstract of each publication.

The string search ended up like this:

((((“Document Title”:classification OR taxonomy OR grouping) AND "Document Title":"authentication techniques" OR "authentication methonds") OR "Abstract":classification OR taxonomy OR grouping) AND "Abstract":"authentication techniques" OR "authentication methonds")

With this only eight results were returned which did not help us a lot to answer the research question. The search string matching was then confined in terms of all the metadata of each publication.

The following search string was used in our case:

((classification OR taxonomy OR grouping) AND ("authentication techniques" OR "authentication methods"))

With this search string 69 results were obtained.

2.2.4 Inclusion Process

The query strings devised in previous section were matched with the titles and abstracts of publications published in the last decade (2002-2013). As a result, the search process returned 69 papers for the three data sources. We read the abstract and introduction of these papers and discarded 45 papers as being irrelevant. The other 25 were retained as relevant for the research. From the resulting 25 papers, four were duplicate publications,

that is, multiple data sources returned the same papers. These duplicates were discarded, leaving 21 papers. two papers were unavailable from the electronic data sources, leaving 18 available full-text papers. We located another 10 papers in other sources such as references from work of related topics or by doing standard internet searches. This included guidelines documents, books, etc. making a total of 29 papers. Of these, 10 were considered irrelevant and 19 papers were selected as being possibly useful for the research.

Finally, these 19 papers where analyzed by reading the entire content in order to decide whether they were of any use for answering the research question. As a result, four papers were considered irrelevant, and only 15 papers (shown on table 1) were found directly related to the classification of authentication techniques.

	Authors	**Title**	**Year**	**Reference**
1	Focardi	Static Analysis of Authentication	2005	(Focardi; 2005)
2	M.Samuel	Enhancing security of Pass Points system using variable tolerance	2010	(M. Samuel; 2010)
3	Mariusz, Piotr, Khalid	User Authentication with Keystroke Dynamics using Fixed Text	2010	(Mariusz, Piotr, Khalid; 2010)
4	Maple, Schetinin	Using A Bayesian Averaging Model for Estimating the liability of Decisions in Multimodal Biometrics	2006	(Maple, Schetinin; 2006)
5	Saxena	Dynamic Authentication: Need than a Choice	2008	(Saxena; 2008)
6	Nosseir, Connor, Revie, Terzis	Question-Based Authentication Using Context Data	2006	(Nosseir,Connor, Revie, Terzis; 2006)
7	Pusara, Brodley	User Re-Authentication via Mouse Movements	2004	(Pusara, Brodley; 2004)
8	Manabe, Fukumoto	AwareLESS Authentication: Insensible Input Based Authentication	2007	(Manabe, Fukumoto; 2007)
9	Asha, Chellappan	Authentication of E-Learners Using Multimodal Biometric Technology	2008	(Asha, Chellappan; 2008)
10	Bhattacharyya, Ranjan, Farkhod, Choi	Biometric Authentication: A Review	2009	(Bhattacharyya, Ranjan, Farkhod, Choi; 2009)
11	Patil, Shimpi	A Graphical Password Using Token, Biometric, Knowledge Based Authentication System for Mobile Devices	2013	(Patil, Shimpi; 2013)
12	NIST	NIST Electronic Authentication Guideline	2011	(NIST; 2011)
13	Hiltgen, Kramp, Weigold	Secure Internet Banking Authentication	2006	(Hiltgen, Kramp, Weigold; 2006)
14	Sethi, Manzoor, Sethi	User Authentication on Mobile Devices	2012	(Sethi, Manzoor, Sethi; 2012)
15	Witte,Rathgeb, Busch	Context-Aware Mobile Biometric Authentication based on Support Vector Machines	2013	(Witte,Rathgeb, Busch; 2013)

Table 1. Classification of authentication techniques references

2.2.5 Exclusion Process

Most of the results excluded, focused on a specific technique instead of the classifications of techniques. Since the word classification is also a term used in Data Engineering, some of the papers were removed because they were about data mining instead of authentication of users. Others were focused on authentication of cyber-attacks, which it is not our focus.

2.3 Results

This section reports the results from the analysis of the fifteen papers detailed in Table 1. First, we give a brief explanation of topics discussed in the paper. Then we identify the different classifications of authentication techniques. Then, we discuss the answers to the stated research question.

Static Analysis of Authentication (Focardi; 2005)

In this paper the author discusses authentication protocols among other things. The entity authentication amounts to reliably agreeing on the claimant identity. The authors classify the authentication techniques in three groups. An important point is made in this book related to this and that is that there techniques that are often combined together to either simplify the use or to be more secure.

The classifications used in this book are:

Something you know
Something you possess
Something inherent

Enhancing security of Pass Points system using variable tolerance (M. Samuel; 2010)

In this Journal article the author talks about Pass Points which is a technique used in authentication using graphical images. As we can see in figure 1, the authentication techniques are classified into three categories in this paper:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Knowledge based authentication is then sub-classified into two different categories:

- Text based authentication
- Picture based authentication

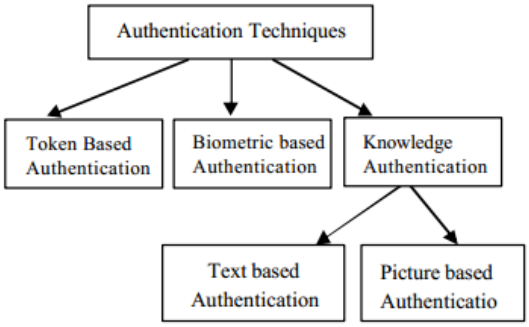

Figure 1. Classification of Authentication Techniques (M. Samuel, 2010)

User Authentication with Keystroke Dynamics using Fixed Text (Mariusz, Piotr, Khalid; 2010)

The proposed approach in this journal article is aimed at efficient user authentication with keystroke dynamics using short fixed text, which may for example occur simultaneously to logging process. The author discusses the state of art in the keystroke dynamics area: definitions, data gathering, extracting, context of keystroke biometrics and most important works in the area. Also present the skeleton of approach proposed by authors, the experimental results and discussion, conclusion and suggested future work. With analysis of only two keystrokes features and with the use of relatively simple classification techniques the keystroke dynamics proved to be promising and effective biometrics for identification/authentication of individuals.

The classifications for authentication techniques used in this article are the following:

- Memory based authentication
- Token-based authentication
- Biometrics based authentication

Using A Bayesian Averaging Model for Estimating the Reliability of Decisions in Multimodal Biometrics (Maple, Schetinin; 2006)

Bayesian Model Averaging (BMA) methodology has been used to allow experts to evaluate the reliability of decisions made in data mining applications. In this journal article it is discussed how the use of Decision Tree models within BMA methodology can be used for a better authentication in multimodal biometric systems.
Here the authors classify Authentication methods into three different categories:

- Token Based (Something you possess)
- Knowledge Based (Something you know)
- Biometrics-Based

Biometrics-Based authentication is then divided into two subcategories:

- Static (Physical attribute)
- Dynamic (Behavioral attribute)

Dynamic Authentication: Need than a Choice (Saxena; 2008)

In this paper the author discuss the various authentication schemes with their pros and cons and present an implemented two factor dynamic onetime password scheme using a mobile device. The author separate password authentication schemes into two: one-war hash function, and public-key based. This based on computation complexity. The author classified authentication upon:

- What someone has (a smart card, token, or ID card),
- What someone knows (a password or PIN)
- What someone is (fingerprint)
- Any combination of these

Question-Based Authentication Using Context Data (Nosseir,Connor, Revie, Terzis; 2006)

In this paper, the authors introduce a question-based authentication scheme appropriate for low risk situations. The authors present an experiment that aimed to investigate whether the histories that smart environments construct of their inhabitants context could also be used to differentiate between genuine users and impostors, as a result they provide a new source of data for authentication schema. Their experiment shows that situations recognized from sensor data can be used to generate questions that differentiate between genuine users and impostors but also that there are a number of issues that need to be addressed before an authentication system based of this kind can be deployed.

The authors make mention that authentication techniques are classified into mechanisms based on:

- Who you are
- Something you carry
- Something you know

User Re-Authentication via Mouse Movements (Pusara, Brodley; 2004)

In this paper the authors present an approach to user re-authentication based on the data collected from the computer's mouse device. The authors make mention that authentication can be achieved by:

- Something the user knows (e.g., access passwords, PIN codes)
- Something the user owns (e.g., access tokens, ID badges, PCcards, smart cards, wireless identification agents)
- Something the user is (e.g., a fingerprint, a palmprint, a voice sample, an iris pattern, which are referred to as biometrics)

AwareLESS Authentication: Insensible Input Based Authentication (Manabe, Fukumoto; 2007)

In this paper the authors propose 'awareLESS' authentication to increase the security of handheld devices. The authors mention that the user can be authenticated by several factors:

- Possession such as IC card and ID tag
- Biological/behavioral characteristics such as fingerprint and gesture,
- Knowledge such as password or PIN.

The authors also make note that possession-based techniques are not secure against theft or loss.

Authentication of E-Learners Using Multimodal Biometric Technology (Asha, Chellappan; 2008)

In this paper the authors discuss E-learning systems authentication using multimodal biometric technology. The authors distinguish the two basic types of biometric systems into:

- Unimodal
- Multimodal biometric system

Each of these systems has some (dis) advantages. A unimodal biometric system is a biometric system using a single biometric feature for person's identification. It is typical to such an approach that this one feature is singled out by means of several technologically distinct methods and systems. Multimodal biometric systems use several biometric features and technologies at the same time.

Biometric Authentication: A Review (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

In this paper the authors give a review on the biometric authentication techniques and some possibilities in the field. A biometric system can provide two functions. One of which is verification and the other one is Authentication. So, the techniques used for biometric authentication has to be stringent enough that they can employ both these functionalities simultaneously. Other biometric strategies are being developed such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor and scent and palm prints. In the near future, these biometric techniques can be the solution for the current threats in world of information security.

The authors classify biometrics into two types:

- Physiological
- Behavior

Physiological systems are considered to be more reliable as individual features of a person, that are used by these systems, do not change by influence of psychoemotional state. Physiological systems of identification deal with statistical characteristics of a person: fingerprints, iris recognition, hand geometry, DNA, face recognition, palm print.
Behavior methods of identification pay attention to the actions of a person, giving the user an opportunity to control his actions. Biometrics based on these methods takes into consideration high level of inner variants (mood, health condition, etc), that is why such methods are useful only in constant use. Behavior or sometimes called psychological characteristics such as voice, gait, typing rhythm are influenced on psychological factors.

A Graphical Password Using Token, Biometric, Knowledge Based Authentication System for Mobile Devices (Patil, Shimpi; 2013)

In this paper the authors discuss how a graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, the authors have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user.

Figure 2 shows the classification provided by the authors into:

- Token Based methods
- Biometric Based methods
- Knowledge Based methods

Biometric Based is then divided into two categories:'

- Contact
- Contact-Less

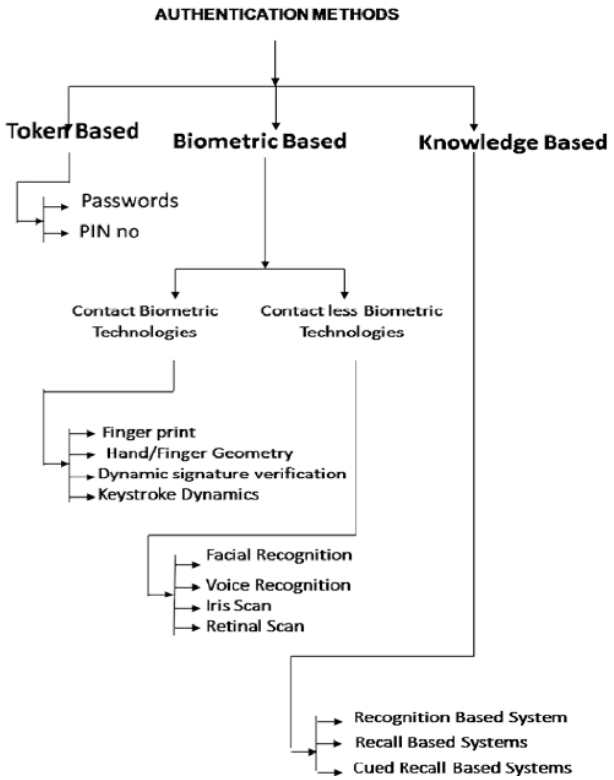

Figure 2. Authentication Methods classification according to (Patil; Shimpi, 2013)

NIST Electronic Authentication Guideline (NIST; 2011)

In this authentication guideline the authors refer to the classic paradigm for authentication systems and that this identifies three factors as the cornerstone of authentication:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a fingerprint or other biometric data)

They also mention that multi-factor authentication refers to the use of more than one of the factors listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.

Secure Internet Banking Authentication (Hiltgen, Kramp, Weigold; 2006)

In this article the authors present two challenge–response Internet banking authentication solutions—one based on short-time passwords and one on certificates—and then describe how easily these solutions can be extended should sophisticated content-

manipulation attacks arise. It describes current authentication threats and two proposed solutions as well as how these solutions can be extended in the face of more complex future attacks.

They classify all Internet banking authentication methods according to their resistance to two types of common attacks*:*

- Offline credential-stealing attacks
- Online channel-breaking attacks

User Authentication on Mobile Devices (Sethi, Manzoor, Sethi; 2012)

In this paper the author discusses how the entity authentication amounts to reliably agreeing on the claimant identity. The author makes an important point that techniques are often combined together to either simplify the use or to be more secure. The author classifies the authentication techniques in three groups as seen in table 2:

- Something you know
- Something you have
- Something you are

	Authentication Factor			Risks Mitigated			Appropriate for Transitions			
	Something You Know	Something You Have	Something You Are	Stolen Device	Borrowed Device	Infected Device	UDUU → UDAU	UDUU → ADUU	UDAU → ADAU	ADUU → ADAU
Authenticating to Server										
2.1.2.1 Require User to Enter Strong Password	●	○	○	●	●	○	●	○	○	●
2.1.2.2 Require User to Enter Weak Password	●	○	○	○	○	○	○	○	○	●
2.1.2.3 Image Based Authentication	●	○	○	○	○	○	○	○	○	●
2.1.2.4 Retrieve Password Stored on Device	○	●	○	○	○	○	○	○	○	○
2.1.2.5 Retrieve another Secret from Device	○	●	○	○	○	○	○	●	●	○
2.1.2.6 Retrieve another Secret from Device (Revocation Capability)	○	●	○	○	○	○	○	●	●	○
2.1.2.7 SMS One-Time-Passwords	○	●	○	○	○	○	○	○	●	○
2.1.2.8 Device-Generated One-Time-Passwords	○	●	○	○	○	○	○	●	●	○
2.1.2.9 Out-of-Band Authentication (Phone Call)	○	●	○	○	○	○	○	●	●	○
2.1.2.10 Hardware Tokens	○	●	○	●	●	○	●	○	○	●
2.1.2.11 Biometrics	○	○	●	●	●	○	●	○	○	●
2.1.2.12 Rely on another Application for Authentication	○	○	○	○	○	○	○	○	○	○

Table 2. Authentication methods divided into different classifications (Sethi; Manzoor; Sethi, 2012)

Context-Aware Mobile Biometric Authentication based on Support Vector Machines (Witte, Rathgeb, Busch; 2013)

In this paper the authors propose a context-aware mobile biometric system. As shown in figure 3 the authors propose a context-aware mobile system in which confidence scores obtained from (biometric) contextual data are used for decision or to parameterize further authentication systems.

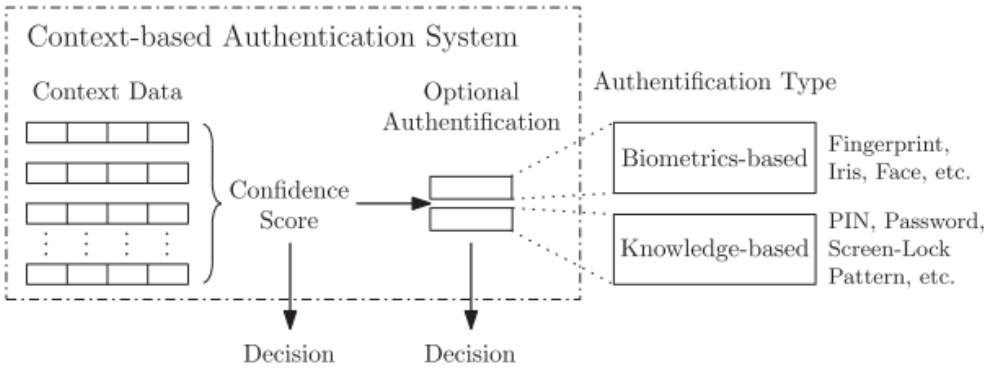

Figure 3. Context-Based authentication system (Witte;Rathgeb; Busch; 2013)

The authors make mention of two classification for authentication methods which are:

- Biometric-Based
- Knowledge Based

2.4 Discussion

In this section we will summarize and consolidate the previous results. We have developed a table, Table 3, to identify which classifications the different authors have managed. In this table we will use numbers to identify the papers as shown on Table 1 in section 2.2.4.

Just by reading the different classifications used in the previous papers we can see that some of them refer to the same concept although use different names. For example Knowledge Based, Something you know, Memory Based, What someone knows, all refer to something a person has to know in order to access the system. We also have: Token Based, Something you have, What someone has, Something you carry, and possession based, something you possess, which basically mean that is something you must have at the time of the authentication to be able to access the system. And also Biometric Based, something you are, what someone is, and who you are, something you inherit all refer to a person's body or personal/biological traits.

Classification	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Knowledge Based		X		X				X			X				X
Token Based		X	X	X							X				
Biometric Based		X	X	X					X	X	X				X
Text Based															
Image Based														X	
Something you know	X			X		X						X		X	
Something you have				X								X		X	
Something you are				X								X		X	
Memory Based			X												
Biometric Based - Static				X											
Biometric Based - Dynamic				X											
What someone knows					X		X								
What someone has					X		X								
What someone is					X		X								
Who you are						X									
Something you carry						X									
Biological								X							
Behavioral								X							
Possession Based								X							
Biometric - Physiological										X					
Biometric - Behavior										X					
Biometric - Unimodal									X						
Biometric - Multimodal									X						
Graphical											X				
Attack Based - offline credential-stealing attacks													X		
Attack Based - online channel-breaking attacks													X		
Contact Less - Biometrics											X				
Contact - Biometric											X				
Something you possess	X														
Something you inherit	X														

Table 3. Summary of authentication techniques classifications A.

In Table 3, we united the values for Knowledge Based, Something you know, Memory Based, What someone knows, into the same row since they all refer to the same thing. For this research we will refer to it as Knowledge based. The values for Token Based, Something you have, What someone has, Something you carry, and possession based, something you possess will be united also and referred to as Token Based for classification purpose. The values for Biometric Based, something you are, what someone is, and who you are, something you inherit will be united as Biometric Based since they all mean the same thing.

Now we have the top three classifications for authentication but there are other classifications left that will be part of the main three. For example for Biometrics we can see

how we have different subclassifications described in the papers: Static, Dynamic, Biological, Behavioral, Phisiological, Behavior, Unimodal, Multimodal. Contactless, and Contact. Just by reading them we can see that Behavioral and Behavior is the same so we can group them together. By reading the definition of what dynamic biometric we can unite it also with the previous two, since they all relate to the actions of a person.

The terms used to describe biometrics where the action of a person is not taken into account but instead are focused on the physical attributes of a person are described by static, biological, or physiological. That is why we are going to group them in the same category 'Static/Physiological'.

The Unimodal and Multimodal classifications relate to whether or not the system is using one (unimodal) or a combination of more than one (multimodal) biometric authentication techniques. Since this is not related to any specific authentication techniques then we decided to discard these two classifications.
The attack based classifications are specific to each individual technique and will require more research going deeper into specific authentication techniques. For this reason attack based classifications will be discarded from our research.

Taking into consideration all of the previous analysis we end up with the classification of authentication techniques described in Table 4. In the appendix a definition of the individual techniques is provided.

Classification	Sub-Classification	Group	Technique
Biometrics-based	Static/Physiological	Contact	Fingerprint
			DNA Analysis
			Finger-knuckle-print (FKP)
			Vascular Patterns
			Palm Print
			Hand Geometry
		Contact-less	Face Recognition
			Body Odor
			Ear Shape
			Retina Scanning
			Facial Thermogram
			Lip Shape
			Iris
	Dynamic/Behavioral	Contact	Keystroke dynamics
		Contact-less	Gait
			Voice
Token Based	Hardware Tokens		Swipe Card
			Key
	Computer/Smartphone		Retrieve Password Stored on Device
			Retrieve another secret from Device
			SMS One time passwords
			Device Generated One Time Passwords
			Out of Band Authentication (Phone Calls)
Knowledge Based	Text Based		PIN
			Login Password
	Image Based		Graphical passwords
	Gesture Based		Pattern Lock (Also considered Graphical)
			Gestural passwords

Table 4. Summary of authentication techniques classifications B.

2.5 Threats to Validity

Until we find other systematic reviews focusing in the usability attributes of authentication techniques we will not be able to validate our study externally.

As for internal validity, the three authors of this research were involved in this systematic mapping study. We discussed and agreed on the procedure and considered activities to counteract the effect of researcher bias. On the search string we used general terms and placed no constraints, in order to better achieve coverage and high accuracy.

The chosen time-frame was intended to include the last decade of research. We also selected some of the most important electronic data sources to which we had access, and added other external sources.

We were particularly careful during the exclusion process, not to discard any potentially interesting paper. For this reason, we also included papers whose abstract or title was not completely clear with respect to our research question for further reading.

3. USABILITY OF AUTHENTICATION TECHNIQUES

3.1 Introduction

In this chapter we first show the definition and attributes of usability that we will be using for our research. Then we will show how our method and procedure of research will be as well as discuss the research question and how we developed our search string. We will discuss what databases we used and how many results we got. Also what our criteria was for eliminating unrelated papers.

We will then show the results and a summary of each related paper and show which usability attributes and authentication techniques they discussed. After all the papers have been summarized and analysed we will then make a discussion based on the usability attributes to show a summary of which authentication techniques have a better usability depending on their usability attributes.

3.2 Definition of Usability

For this thesis we will use Usability as the definition of Operability and Usability based on ISO/IEC 25010 (SQuaRE).
Operability is defined as the degree to which the product has attributes that enable it to be understood, learned, used and attractive to the user, when used under specified conditions.

- **Appropriateness recognisability** is defined as the degree to which the product provides information that enables users to recognize whether the software is appropriate for their needs.
- **Learnability** is defined as the degree to which the product enables users to learn its application.
- **Ease of use** is defined as the degree to which users find the product easy to operate and control.
- **Attractiveness** is defined as the degree to which the product is attractive to the user .
- **Technical accessibility** is defined as the degree to which users with specified disabilities can operate the product.
- **Operability compliance is defined as** the degree to which the product adheres to standards, conventions, style guides or regulations in laws and similar prescriptions relating to operability.

Usability is defined as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

- **Effectiveness** is defined as the accuracy and completeness with which users achieve specified goals
- **Efficiency** is defined as the resources expended in relation to the accuracy and completeness with which users achieve goals.
- **Satisfaction** is defined as the degree to which users are satisfied in a specified context of use.

  Satisfaction can be further subdivided into the following sub-subcharacteristics.

  - Likability is cognitive satisfaction
  - Pleasure is emotional satisfaction
  - Comfort is physical satisfaction
  - Trust is satisfaction with security

- **Usability compliance** is defined as the degree to which the product adheres to standards or conventions relating to usability

3.3 Research Method and Procedure

This section presents the process enacted to conduct our systematic mapping study of the literature related to the usability attributes of authentication techniques. Similarly to section, 2.2, the guidelines provided by Petersen et al. (2008) were used to build this systematic map.

3.3.1 Research Question

There are many authentication techniques used today, in order to facilitate their study we formulated the following research question:

RQ: How do the different authentication techniques classifications compare in terms of the usability attributes?

This question intends to clarify the different classifications that exist for the different authentication techniques available today. Once we have the answer to this question we will extend the mapping study to the different authentication methods and their usability.

3.3.2 Search Strategy

The search was run on several well-known databases, such as IEEE Xplore, ACM Digital Library, and DOAJ (Directory of Open Access Journals), as well as some individual journals and papers.

The publication year was set between 2002 and 2013 to limit the results to documents published within the last 11 years. Then, the titles and the abstracts of the identified articles were checked against set eligibility and relevance criteria (this criterion is explained in Section 3.3.4).

3.3.3 Data Retrieval

In order to collect information that could be used to answer the research question; search strings were devised. If the database allows it the Boolean operators AND and OR were used to do the search. The OR operator allows to include alternative words or synonyms and the AND operator allows to unite two or more words or phrases together.

X was composed of synonyms of or words possibly related to classification

X: ("usability" OR "efficiency" OR "satisfaction" OR "learnability" OR "recognisability" OR "memorability" OR "ease of use" OR "attractiveness")

Y was composed of synonyms of or words possibly related to authentication techniques, using each linked by the “OR” operator.

Y: {Authentication techniques OR authentication methods}

Finally, the “AND” operator was added between X and Y to retrieve relevant literature related to classification of authentication techniques. Search string matching was confined to terms in the title and abstract of each publication.

The following search string was used in our case:

> ("usability" OR "efficiency" OR "satisfaction" OR "learnability" OR "recognisability" OR "memorability" OR "ease of use" OR "attractiveness") AND ("authentication techniques" OR "authentication methods")

The string includes memorability even though it is not specifies as an usability attribute for the ISO/IEC 25010 (SQuaRE) since it is how well the user remembers, in this case a password or something to get authenticated. We have to make sure the papers that we chose talk about the user remembering that which he/she needs to get authenticated and not the actual software or program remembering.

We eliminated other attributes such as: technical accessibility, operability compliance, and effectiveness since they did not add value to the purpose of this research.

3.3.4 Inclusion Process

The query strings devised in previous section were matched with the titles and abstracts of publications published in the last decade (2002-2013). As a result, the search process returned 309 papers for the three data sources. We read the abstract and introduction of these papers and discarded 232 papers as being irrelevant. The other 77 were retained as relevant for the research. From the resulting 77 papers, four were duplicate publications,

that is, multiple data sources returned the same papers. These duplicates were discarded, leaving 73 papers. Two papers were unavailable from the electronic data sources, leaving 71 available full-text papers. Of these, 32 were considered irrelevant and 39 papers were selected as being possibly useful for the research.

Finally, these 39 papers where analyzed by reading the entire content in order to decide whether they were of any use for answering the research question, most because they talked about usability in general but not in terms of its attributes and were not part our scope, others because they focused on usability for certain disabilities. As a result, 25 papers were considered irrelevant, and only 14 papers (Table 5) were found directly related to the usability attributes of authentication techniques.

Authors	Title	Year	Reference
Ma, Feng	Evaluating Usability of Three Authentication Methods in Web-Based Application	2011	(Ma, Feng; 2011)
Hamilton, Carlisle, Hamilton Jr.	A Global Look at Authentication	2007	(Hamilton, Carlisle, Hamilton Jr.; 2007)
Forget, Chiasson, Biddle	Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords	2010	(Forget, Chiasson, Biddle; 2010)
Ritter	MIBA: Multitouch image-based authentication on smartphones	2013	(Ritter; 2013)
Luca	Eyepass - eye-stroke authentication for public terminals	2008	(Luca; 2008)
Braz, Robert	Security and Usability: The Case of the User Authentication Methods	2006	(Braz, Robert; 2006)
Schlöglhofer, Sametinger	Secure and Usable Authentication on Mobile Devices	2012	(Schlöglhofer, Sametinger; 2012)
Tari, Ozok, Holden	A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords	2006	(Tari, Ozok, Holden; 2006)
Schaub, Walch, Könings, Weber	Exploring the Design Space of Graphical Passwords on Smartphones Graphical Passwords on Smartphones	2013	(Schaub, Walch, Könings, Weber; 2013)
Spitzer, Singh, Schweitzer	A Security Class Project In Graphical Passwords.	2010	(Spitzer, Singh, Schweitzer; 2010)
Riley, McCracken, Buckner	Fingers, Veins and the Grey Pound: Accessibility of Biometric Technology	2007	(Riley, McCracken, Buckner; 2007)
Trewin, Swart, Koved, Martino, Singh, Ben-David	Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption	2012	(Trewin, Swart, Koved, Martino, Singh, Ben-David; 2012)
Zezschwitz, Dunphy, De Luca	Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices	2013	(Zezschwitz, Dunphy, De Luca; 2013)
El-Abed, Giot, Hemery, Rosenberger	A study of users' acceptance and satisfaction of biometric systems	2010	(El-Abed, Giot, Hemery, Rosenberger; 2010)

Table 5. Usability attributes of authentication techniques references

3.4 Results

This section reports the results from the analysis of the fourteen papers detailed in table 5. We give a brief explanation of what are the topics discussed in the paper. Then we identify parts that might help us identify the usability attributes of some authentication techniques. Then, we discuss the answers to the stated research question.

Evaluating Usability of Three Authentication Methods in Web-Based Application (Ma, Feng; 2011)

In this paper the authors evaluated three authentication methods: traditional text password, Mnemonic password, and graphical password.
For authentication time, the authors concluded text based authentication is better than graphical based authentication. The authentication time consumed mainly depended on the authentication key size and the number of authentication pages. Since images have bigger size than text, the key transfer between server and client would use more time for graphical based authentication when the network transfer speed rate is certain.
Regarding the memorability feature, the authors measured it by logging failure rate. Passwords had a login failure rate of 15.1%, while Passfaces for the same participants produced a login failure rate of 4.9%. 90% participants succeed in the authentication process using the Déjà Vu method, but only 70% succeed using the text password under the same condition. More recently, Tullis et al. evaluated the memorability of graphical passwords and found that users can still remember their graphical passwords after six years. However, the images used for passwords were provided by the participants themselves, which significantly improved memorability because additional cues existed in those images. In reality, it may not be feasible to have the users contributing the password images.

Considering ease of use, usernames and passwords are relatively ancient technology and it is really easy to use by people. The graphical passwords are recently emerged authentication methods. To date there is no reported empirical studies that evaluate the ease of use of the major types of authentication methods in a real life setting during prolonged period of time. The work load of choosing a text, serial pictures, or serial points in a picture has not been measured in existing research. This study aims to address that gap and provide systematical evaluation of the usability of three authentication methods: text password, mnemonic password, and recognition-based password.

They conducted a longitudinal empirical study to investigate the usability of three authentication methods in a real life web based environment.. The result suggested that graphical passwords took longer time than the text password and mnemonic password. The text passwords and graphical passwords are equally memorable. The mnemonic passwords resulted in higher average failure rate than the other two types of passwords. Overall, the graphical passwords demanded higher work load than the text passwords and the mnemonic passwords. This study is a preliminary evaluation of the three authentication methods because the sample size is rather small. In future research, we will examine substantially larger sample size to confirm the findings. We are also planning to study

whether there is difference in performance and work load when the authentication methods are used by diversified user population such as people with cognitive disabilities or elder users.

A Global Look at Authentication (Hamilton, Carlisle, Hamilton Jr.; 2007)

In this paper the authors discuss some authentication techniques from a security point of view and also about their usability in general. The following techniques were discussed:

-Password: The user has to remember the password and it might have a restriction on the minimum number of characters.

-Smartcards: The downside is that users may need to carry more than one smartcard and it can get lost and will have to be replaced costing the user money.

-Biometrics: User does not have to remember any kind of PIN or password. Small changes may in fact create a false match or nonmatch. A system that needs high security will have a low false match rate, which reduces the tolerance of the system. The overhead of the system rejecting valid users may be acceptable due to the sensitivity of the information. They can be very secure but there exists the problem of initial enrollment and setup of these systems. Numerous entities exist for an individual to have to authenticate, and setting up identification means with each individual entity would be time consuming, and difficult to manage.

Behavioral Authentication: Does not require the user to remember anything specific, or physically carry a smartcard or key that gives them access to the system. It is also advantageous over biometrics, because behavior authentication is not likely to require additional hardware to implement. It cannot be used as primary authentication due to the requirement to track multiple user actions over time instead of the instantaneous authentication that a password or key can provide.

Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords (Forget, Chiasson, Biddle; 2010)

This paper refers to Graphical passwords and that they are proposed as more memorable and secure authentication methods that leverage the human ability to more easily recognize and recall images over text. Which refers to memorability. One disadvantage to most graphical password schemes is their susceptibility to shoulder-surfing: attackers may observe or record users as they enter passwords and subsequently log in with the observed credentials.

MIBA: Multitouch image-based authentication on smartphones (Ritter; 2013)

In this paper the author proposes MIBA as an image-based authentication method. It is discussed here the usability of both text based password and graphical passwords. For text based password it mentions that entering text-based passwords on virtual keyboards is more tedious compared to physical keyboards due to varying typing effort for characters from different categories (lowercase/uppercase characters, numbers, special characters). This is especially apparent for passwords containing special characters, which can require up to three taps for entry due to navigation of additional keyboard pages. As an alternative to text-based passwords, graphical authentication methods have emerged. Instead of characters, a graphical password consists of a number of graphical elements or patterns that the user selects or draws on the screen. It also mentions that nowadays, graphical passwords are already being employed on smartphones to unlock the screen, e.g., the Android Pattern Lock based on Pass-Go. Graphical passwords promise higher usability and better memorability of passwords.

Eyepass - eye-stroke authentication for public terminals (Luca; 2008)

In this paper the author presents EyePass, an authentication mechanism based on PassShape and eye-gestures. In this paper the author also analyzes passwords and PINS authentication with surveys. A short survey was conducted and showed that 59 out of 88 participants (55,7%) had forgotten a PIN with the consequence that their access to a specific service was locked by the service provider. Indicating a bad memorability in comparison with biometrics authentication such as Eyepass. The authors assumed that many humans have problems memorizing abstract number sequences and complex passwords used for current authentication purposes.

Security and Usability: The Case of the User Authentication Methods (Braz, Robert; 2006)

As part of this project, the authors developed a comparative analysis of the different features encountered in authentication methods according to Table 6 and Table 7. To describe the following features they make use of subjective rating scales: "Security" and "Usability" (ranging from 1=Minimum to 5=Maximum in order to measure the degree of severity issues related to each authentication method). The usability in this case will be classified as ease of use.

Feature/ Acquisition Device	Pass-words (PW)	PIN	Prox-imity card	One Time Gener ators	Chal-lenge Re-sponse	Multi func-tion card	Pub-lic Key (PK)	Ker-beros	Finger print or Hand or Face	Voice	Sig-nature	Ret-ina/ Iris	Key-stroke Rec-ogni-tion	Un-der-the-skin ID chip
Definition	Know ledge based 8 to 12 digits	Know ledge based 4 dig-its	Authe ntica-tion Token	Authe ntica-tion Token	Authe ntica-tion Token	Authe ntica-tion Token	Cryp-togra-phy (PK and PRK)	Key Distri-bution Center	Bio-met-rics User scan-ning	Bio-met-rics User voice when speak ing	Bio-met-rics Lengt h-/widt h pen pres-sure	Bio-met-rics Pat-tern of blood vessels	Bio-met-rics User's typ-ing rhyth m	RFID based
Advantages	Ease of de-ploy-ment	Net-work-less	Last longer (con-tact-less)	PW diffi-cult to guess	No syn-chro-niza-tion	Built-in dy-namic data proc-essing	User credent ials once per login session	Mu-tual Authe ntica-tion	Ease to col-lect	No PWs	High defi-nition graph ic	Un-chang eable (life-time)	No enrol-ment	Forger, steal chip is pretty hard
Disadvan-tages	Can be for-gotten	Can be for-gotten	Theft, fraud, coun-terfeit	Brute force, dic-tion-ary attack	Users shares their ac-cess permi ssions	Need of a smart card reader	PK is single point of at-tack	Scal-abil-ity	Crimi nal affilia tion	Chan ges over time	Can change signa-ture at any time	Exces sive user coop-era-tion	Mas-quer-ade (spoof ing)	Mas-quer-ade (spoof ing)
Security	2	2	3	3	3	5	5	5	4	1	3	5	3	4
Usability	2[1]	2	3	3	3	3	3	3	3	5	3	2	3	3

Table 6. Comparative Analysis of the Authentication Methods. (Braz, Robert; 2006)

Feature/ Acquisition Device	Voice	Prox-imity card	Finger print or Hand or Face	Key-stroke Rec-ogni-tion	Un-der-the-skin ID chip	Sig-nature	Ret-ina/ Iris	Pass-words (PW)	PIN
Usability	5	3	3	3	3	3	2	2[1]	2

Table 7. Comparative Analysis of the Authentication Methods simplified. (Braz, Robert; 2006)

Secure and Usable Authentication on Mobile Devices (Schlöglhofer, Sametinger; 2012)

In this paper the authors discuss the usability and authentication on mobile devices. They mention that usability of modern mobile devices is influenced by the use of touch screens and the duration of the time it takes to unlock the device. Additionally, they evaluate the complexity, i.e., how much users have to remember in order to successfully authenticate, as well as the reliability of the system.

Touch screen. The usability of PINs and especially passwords is limited in the context of mobile devices, mainly because mobile devices are typically equipped with a touch screen rather than a hardware keyboard like traditional computers. Virtual keyboards are inconvenient to enter secure passwords, which ideally contain a variation of uppercase and lowercase letters, digits and special characters. The Android unlock pattern, GesturePuzzle

and, thus, SecureLock are better suited for authentication via touch screen. NFC tags are independent from screen and keyboard.

Duration. The duration of the authentication process is crucial for user acceptance. We roughly estimate 4 sec to enter a PIN and 10 sec to enter an average password. The unlock pattern and Face Unlock take less than a PIN. The Android unlock pattern is only secure if it uses a long path. But the longer the pattern, the more time is needed for authentication, again resulting in reduced usability. Therefore, most users prefer rather short patterns, so that the authentication can be carried out within a short period of time. GesturePuzzle takes a little longer than the unlock pattern because users have to analyze the images in the relevant area. Use of an NFC tag will take 2-5 sec, depending on where the tag is carried and how easily accessible it is. As SecureLock combines GesturePuzzle and NFC tags it will take a little longer. We estimate 5- 8 sec which is less than the input of an average password.

Complexity. Images are typically much better to remember for humans than text, unless the text is short like a four-digit PIN. Unlock patterns may get quite complex unless it is a simple and insecure circle or square. The same holds for GesturePuzzle with the additional burden that more than one pattern has to be remembered in addition to sets of images.

Reliability. Android´s Face Unlock is promising but still struggling with usability problems. For example, faces of people with dark skin are not always recognized. For authentication, the front camera of the smart phone, which has no flash light, is used. Therefore, faces in low light are not correctly recognized.

Table 8 summarizes their usability perceptions. Expectedly, PINs and NFC tags do quite well. SecureLock's rating has circles for duration and complexity, the price that had to be paid for security. NFC tags do best in usability, closely followed by unlock patterns.

	PIN	Password	Unlock Pattern	Face Unlock	GesturePuzzle	NFC Tags	SecureLock
Touch Screen	o	-	✓	✓	✓	✓	✓
Duration	✓	-	✓	✓	✓	✓	o
Complexity	✓	-	o	✓	o	✓	o
Reliability	✓	✓	✓	-	✓	✓	✓

Table 8. Comparison of Usability Aspects (Schlöglhofer, Sametinger; 2012)

A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords (Tari, Ozok, Holden; 2006)

This paper examines the real and perceived vulnerability to shoulder-surfing of two configurations of a graphical password, Passfaces™, compared to non-dictionary and dictionary passwords.

Passwords/PINS **:** A number of studies have documented the problem that most users cannot remember a unique set of authenticators and identifiers for each of the systems they use. These authors typically cite basic human cognitive limitations from the psychology literature in explaining why this is so. For example, one issue is the amount of memory burden put on the users relating to the chunking principle by Miller. This is especially true when organizations (typically employers) require employees to create "strong passwords" that are less susceptible to dictionary and brute force attacks.

Graphical Passwords**:** Graphical passwords rely on a user to select a predetermined image or set of images on a visual display (like a Web browser or PDA screen) by selecting those images in a particular order to authenticate the user. Claims of enhanced usability from graphical passwords derives from humans' innate ability to recognize faces, which machines have been trying to emulate with mixed success for some time now.

Brostoff and Sasse conducted some of the first empirical research on Passfaces™ and found a significantly lower rate of password resets and higher levels of memorability compared to passwords in a comparative test spanning over five months. They also found that performance was slower than for passwords, in part because users had to pass through a number of screens with faces and also because of the relatively out-of-date hardware and software platforms used for the experiments. However, this research did confirm the presumed increase in memorability of graphical passwords compared to alphanumeric passwords. Subsequent research has replicated this relatively slower performance time for graphical versus alphanumeric passwords, with mixed results on memorability and ease of use.

Exploring the Design Space of Graphical Passwords on Smartphones (Schaub, Walch, Könings, Weber; 2013)

In this paper the authors analyze and describe this design space of graphical passwords. In the process, they identify and high-light interrelations between usability and security characteristics, available design features, and smartphone capabilities.

They mention that graphical authentication mechanisms have the potential to overcome certain issues with text-based passwords, such as password memorability and the lack of recall cues, because visual representations are more memorable and easier to recall.

They find that graphical passwords are not effort-less in terms of memorability but offer advantages over text-passwords as images can be used as cues for different pass-words. They further point out that graphical passwords are easy to learn, but typically require

longer entry times than text passwords at least in the web and desktop context. They also note that graphical passwords have low accessibility, because they rely on the recognition of and interaction with visual elements.

A Security Class Project In Graphical Passwords. (Spitzer, Singh, Schweitzer; 2010)

In this paper the authors detail the development and implementation of a research project. The purpose of the project is to teach students in-depth knowledge about a security topic and provide a research experience.

Over 50 users used our graphical password system and provided feedback on its usability and memorability. Figure 8 shows the results of a survey asking participant show easy the system was to use. The average rating was 3.8 on a scale of 1 to 5. Individual comments included the fact that it took longer to click a sequence of grid locations than simply typing a password, and that the image size should be adjustable to allow for easier navigation when clicking.

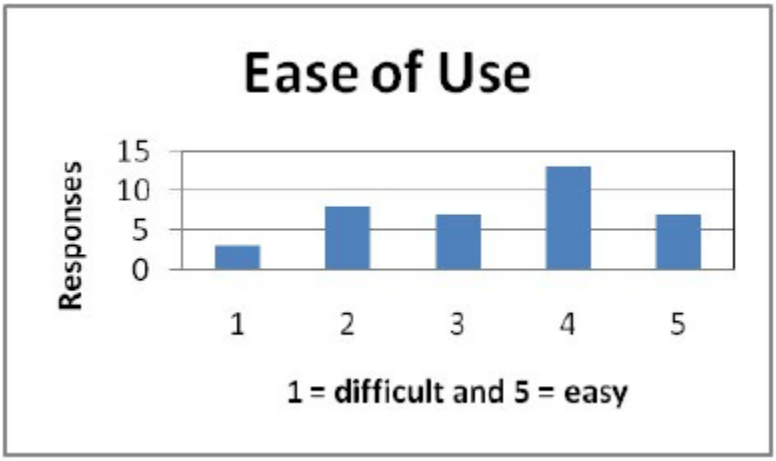

Table 9. User survey on system's ease of use. (*Spitzer, Singh, Schweitzer; 2010*)

In terms of memorability, 60% of the users rated the system as easier to remember than alphanumeric, while 40% said it was more difficult. One suggestion for improving usability was to allow the user to go back one level to change the sequence versus having to reset and start from the beginning. User feedback of this approach is that it is easy to use. However, the fact that 40% indicated it was harder to remember than alphanumeric indicates that it is not, in its current form, ready to replace traditional authentication techniques. A larger user study is necessary to exercise the system and collect quantifiable information on the effect of different levels, and ways to improve the user interface.

Fingers, Veins and the Grey Pound: Accessibility of Biometric Technology (Riley, McCracken, Buckner; 2007)

In this paper the authors investigated both the accessibility and acceptability of biometric technology for an older population. They mention that Fingerprint verification systems are the most widely used biometric technology; however several studies suggest that their performance deteriorates when older individuals use the technology. This research investigated both the accessibility and acceptability of biometric technology for an older population.

Technology Preference: Participants preferred vein over fingerprint technology. The vein technology was rated as easier to use, faster, and less stressful than the fingerprint system. Participants reported that they would be more willing to use vein based biometrics at an ATM than fingerprint technology. These differences are summarized below in figure 4 below. There was a relationship between participant age and device preference, with older participants preferring the vein based system. This effect is explained by the superior performance of the vein system with older users.

Ease of use	Vein > Fingerprint
Speed of use	Vein > Fingerprint
Security	Vein = Fingerprint
Stressfulness	Vein > Fingerprint
Preference	Vein > Fingerprint
Willingness to use	Vein > Fingerprint

Figure 4. Relationships between opinion measures for the fingerprint

Correspondence of Usability Measures: It is interesting to investigate the correspondence between the different measures of usability collected here. In general subjective measures correspond with willingness to use the technology to a greater extent than objective measures of usability. There was no relationship between verification times or verification performance with measures of user opinion. The only objective measure that was related to preference was fingerprint FTE rate. Enrolment rate was negatively correlated with preference for the fingerprint device. Perceived ease of use correlated with willingness to use and preference for both the fingerprint and vein systems. There was a relationship between perceived security of the technology and willingness to use, but not with security and device preference. There was a weak relationship between willingness to use the technology and device preference. These relationships are shown in Figure 5 below.

	Security		Willingness to use		Preference	
Ease of use	Fingerprint	$r_s = .07$	Fingerprint	$r_s = .41$*	Fingerprint	$r_s = .67$ **
	Vein	$r_s = .06$	Vein	$r_s = .49$**	Vein	$r_s = .41$ *
Security			Fingerprint	$r_s = .49$ **	Fingerprint	$r_s = .01$
			Vein	$r_s = .43$ *	Vein	$r_s = -.05$
Willingness to use					Fingerprint	$r_s = .39$ *
					Vein	$r_s = .26$

Figure 5. Relationships between subjective measures for fingerprint and vein technology. All relationships were calculated using Spearman's correlation coefficient. * Correlation significant at 0.05 level. ** Coloration significant at 0.01 level. (Riley, McCracken Buckner; 2009)

Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption (Trewin, Swart, Koved, Martino, Singh, Ben-David; 2012)

The authors examined three biometric authentication modalities – voice, face and gesture – as well as password entry, on a mobile device, to explore the relative demands on user time, effort, error and task disruption.
This study was the first to measure user action times for authentication using different biometrics on a mobile device. It provides insight into user performance when using these techniques under favorable conditions.

The study examined:

1. The time taken to provide an authentication sample (password, biometric, or two biometrics); 2. Error rates in providing a sample of suitable quality for analysis by verification algorithms; 3. The impact of the user actions required for authentication on performance in a memory recall task; and 4. User reactions to the authentication methods.
In table 10 and table 11 below are the summaries for memory task performance and for System Usability Scale.

Condition	Memory task preparation time (median sec)	Memory task (% success)
Password	4.3	73
Voice	5.4	76
Face	3.9	85
Gesture	4.2	72
Face+Voice	5.3	71
Gesture+Voice	5.7	65

Table 10. Memory task performance summary (Trewin, Swart, Koved, Martino, Kapil Singh, Ben-David; 2012)

Condition	SUS score	SUS response percentile (approx.)	SUS grade	Fatigue
Password	78%	80^{th}	C	2.5
Voice	66%	40^{th}	D	3.0
Face	75%	76^{th}	C	2.2
Gesture	77%	78^{th}	C	2.4
Face+Voice	46%	8^{th}	F	3.7
Gesture+Voice	50%	13^{th}	F	3.8

Table 11. System Usability Scale summary (Trewin, Swart, Koved, Martino, Kapil Singh, Ben-David; 2012)

Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices (Zezschwitz, Dunphy, De Luca; 2013)

In this paper, the authors presented the results of a field study, in which they evaluated performance, usability and likeability aspects of Android-like graphical passwords in the wild in comparison with PIN. In addition, they presented a taxonomy that helps to get further insights into the origins of logged errors. By evaluating Android-conform patterns, they gathered generalizable results, while the evaluation of their more complex counterparts provided insights into the effects of allowing a non-restricted password space.

The study revealed that one main difference of both approaches is the concept of error recovery. While the PIN prototype allows for recovering from errors using undo operations, the pattern users were forced to submit every attempt without corrections. This is the same approach that is found in current real world implementations. The results show that input speed and success rate were influenced by the concept of error recovery. While the average input speed of PIN users was significantly faster, we could show that using undo operations had a significant effect on the input speed as well. Thus, the average time of authentications, where such operations were used, were significantly slower, even compared to sessions using the pattern approach. Using our taxonomy revealed that most of the errors of the pattern group were based on slips and thus, one could assume that a lot of these errors could have been avoided using undo operations. However as mentioned above, undo operations were not supported by the pattern prototype. Even if they could have been avoided, based on our qualitative findings, it is doubtful that they would have been avoided very often.

The findings revealed that significantly more participants of the pattern group stated that recovering from errors was fast or very fast. In addition, the pattern prototype users were not irritated by the number of failed attempts as likeability ratings benefited the pattern prototype as well. This leads to the conclusion that fast error recovery is more important for the users than error avoidance and questions the benefit of undo operations for such an approach.

A study of users' acceptance and satisfaction of biometric systems (El-Abed, Giot, Hemery, Rosenberger; 2010)

In this paper the authors describe the evaluation aspects of biometric systems: performance, acceptability and satisfaction, data quality and security. The summary of Face System and Keystroke system can be seen in the table 12 below. For this research we will focus on the 'easy to use' part of the table.

Perception questions	*Face system*	*Keystroke system*	*p-value*
Disturbed	1.8	1.54	0.05
Threats to privacy	2.33	1.52	<< **0.05**
Easy to use	3.41	3.39	0.96
Verification fast	3.46	3.47	0.68
Correct answer	3.36	3.72	**0.01**
System can be easily attacked	2.6	2.38	0.22
Use in the future	3.06	3.2	0.23
Trust	2.96	3.03	0.7
General appreciation	2.98	3.26	**0.02**

Table 12. Comparative analysis of perception between the studied systems, kruskall-wallis analysis (El-Abed, Giot, Hemery, Rosenberger; 2010)

In their study the authors concluded that for Ease of Use in Face Time and Keystroke system have relative the same ease of use.

3.5 Discussion

This section will be divided into several parts. First we will summarize, analyze, and group together the papers based on the usability attribute they deal with. With this we will be able to see which authentication technique has a better usability in terms of a specified attribute. During this process we have found some papers with conflicting conclusions, so we will study them separately. We also found that some of the usability attributes were not study in literature, we will discuss them.

Some usability attributes and authentication techniques have been studied more than others so some attributes will have more information than others. The same goes for some of the authentication techniques.

3.5.1 Usability attributes under agreement

In this section we will group the papers based on the usability attributes they study. Then we will summarize which authentication techniques have a better usability based on those attributes.

Memorability

Table 13 shows a summary of how memorability has been considered in literature. In Table 13, we can see several studies that confirm that Graphical authentication has a better memorability than Text based authentication. This mainly seems to be because users have an easier time remembering images. Also the images that they have to remember in most cases are selected by them. We can also see how Iris scan has a better memorability than a PIN number, since iris scan does not require the user to actually remember anything.

Paper	Technique	Classification	Comparison	Other Technique
(Ma, Feng; 2011)	Graphical	Knowledge Based	better than	text based
(Forget, Chiasson, Biddle; 2010)	Graphical	Knowledge Based	better than	text based
(Ritter; 2013)	Graphical	Knowledge Based	better than	text based
(Schlöglhofer, Sametinger; 2012)	Graphical	Knowledge Based	better than	text based
(Tari, Ozok, Holden; 2006)	Graphical	Knowledge Based	better than	text based
(Schaub, Walch, Könings, Weber; 2013)	Graphical	Knowledge Based	better than	text based
(Spitzer, Singh, Schweitzer; 2010)	Graphical	Knowledge Based	better than	text based
(Luca; 2008)	Iris Scan	Biometrics	better than	PIN number
Comparison Based on Classifications				
(Hamilton, Carlisle, Hamilton Jr.; 2007)		Token Based	better than	knowledge based
		Biometrics	better than	knowledge based
		Behavioral	better than	knowledge based

Table 13. Summary of authentication techniques comparison based on the memorability attributes according to research.

Other authors have studied memorability in general for the three main classifications of authentication techniques. Those authors have found that Token based authentication and Biometrics have a better memorability than Knowledge based authentication (since users do not have to memorize anything). Inside Biometrics we also have behavioral authentication which also has a better memorability than knowledge based authentication. This is summarized on Table 14 below. We used the positive symbol (+) and green color to show that it has better memorability and the negative symbol (-) and orange color to show which authentication technique has less usability in terms of the specified usability attribute. In the case of equal authentication the equal symbol (=) and the color yellow were used.

Memorability	
Graphical Authentication	Text Based Authentication
+	-
Based on Classifications	
Biometrics Based	Knowledge Based
+	-
Behavioral Auth.	Knowledge Based
+	-
Token Based	Knowledge Based
+	-

Table 14. Memorability comparison

Satisfaction

For the satisfaction attribute, in Table 15 we summarize the results found in literature. From this table we can also get that both PIN authentication and Graphical authentication have a better satisfaction than text based authentication. Also vein authentication has a better satisfaction than Fingerprint authentication.

Paper	Technique	Classification	Comparison	Other Technique
(Schlöglhofer, Sametinger; 2012)	PIN	Knowledge Based	better than	text based
	Graphical	Knowledge Based	better than	text based
(Riley, McCracken, Buckner; 2007)	Vein	Biometrics	better than	fingerprint

Table 15. Summary of authentication techniques comparison based on the satisfaction attributes according to research.

This is summarized on table 16 below.

Satisfaction	
PIN Authentication	Text Based Authentication
+	-
Graphical Authentication	Text Based Authentication
+	-
Vein Authentication	Fingerprint Authentication
+	-

Table 16. Satisfaction comparison

Efficiency

For the efficiency attribute we can see how based on our research text based authentication is better than graphical authentication since it usually takes less time to authenticate, as seen on table 17 below.

Paper	Technique	Classification	Comparison	Other Technique
(Ma, Feng; 2011)	Text based	Knowledge Based	better than	Graphical authentication

Table 17. Summary of authentication techniques comparison based on the efficiency attributes according to research.

The summary of efficiency is on table 18 below.

Efficiency	
Text Based Authentication	Graphical Authentication
+	-

Table 18. Efficiency Comparison

Ease of Use

As we can see on Table 19 below, the Ease of Use usability attribute has been the one we found more of in our research. We found that Behavioral techniques have a better ease of use than any other authentication technique out there. It has a better ease of use than: Static Biometrics Based Authentication Techniques, Knowledge based authentication techniques, and token based authentication techniques. This happens in part because users don't have to do anything other than what they would normally do.

Vein technology was found to have a better ease of use of than fingerprint technology. The participants of this research preferred vein over fingerprint technology. The vein technology was rated as easier to use, faster, and less stressful than the fingerprint system.

Keystroke has better ease of use than knowledge based techniques and same ease of use as face authentication techniques. Based on the developed comparative analysis of the authors on different features encountered in authentication methods, Voice recognition has better ease of use than knowledge based technologies. This also based on a comparative analysis. Fingerprint/Hand/Face Recognition (Biometrics) technologies have better ease of use than knowledge based technologies. Proximity Card Authentication has the same ease of use as fingerprint, hand, face, keystroke, and iris. All of them based on a comparative analysis.

Text password and PIN password have the same ease of use. However they have worst ease of use than biometrics and Token based technologies. Iris recognition has better ease of use than Knowledge based technologies. This happens in part because in biometrics and

in token based authentication users usually have less interaction with the system in comparison to knowledge based authentication.

Lastly Pattern authentication has a better ease of use than PIN based authentication. This based on the results of a real world user study across 21 days that was conducted; where they compared the performance of Android-like patterns to personal identification numbers (PIN), both on smartphones, in a field study.

Paper	Technique	Classification	Comparison	Other Technique
(Braz, Robert; 2006)	Card	Token Based	same as	Fingerprint/Hand/Face
	Fingerprint/ Hand/Face	Biometrics	better than	knowledge based
	Iris	Biometrics	better than	knowledge based
	Keystroke	Biometrics	better than	knowledge based
(El-Abed, Giot, Hemery, Rosenberger; 2010)	Keystroke	Biometrics	same as	facetime
(Braz, Robert; 2006)	Password	Knowledge Based	worse than	biometrics, token
(Zezschwitz, Dunphy, De Luca; 2013)	Pattern	Knowledge Based	better than	PIN based authentication
(Braz, Robert; 2006)	PIN	Knowledge Based	worse than	biometrics, token
(Riley, McCracken, Buckner; 2007)	Vein	Biometrics	better than	fingerprint
(Braz, Robert; 2006)	Voice	Biometrics	better than	knowledge based
Comparison Based on Classifications				
(Hamilton, Carlisle, Hamilton Jr.; 2007)		Behavioral	better than	biometrics, knowledge, token

Table 19. Summary of authentication techniques comparison based on the ease of use attributes according to research.

Table 20 below shows a summary of the Ease of use attribute and the authentication techniques.

Ease of Use	
IRIS Authentication	Knowledge Based Auth.
+	-
Keystroke Authentication	Knowledge Based Auth.
+	-
Fingerprint Authentication	Knowledge Based Auth.
+	-
Hand Authentication	Knowledge Based Auth.
+	-
Face Authentication	Knowledge Based Auth.
+	-
Proximity Card	Fingerprint/Hand/Face/ Signature/Keystroke
=	=
Proximity Card	Knowledge Based Auth.
+	-
Keystroke Authentication	Face Authentication
=	=
Biometrics Based	Text Based Authentication
+	-
Token Based	Text Based Authentication
+	-
Pattern Based Auth.	PIN Based Authentication
+	-
Biometric Based	PIN Based Authentication
+	-
Token Based	PIN Based Authentication
+	-
Vein Authentication	Fingerprint Authentication
+	-
Voice Authentication	Knowledge Based
+	-
Classification Based	
Behavioral	Static Biometrics Based / Knowledge Based / Token Based
+	-

Table 20. Ease of Use Comparison

3.5.2 Conflicting usability

In this section we will discuss conflicting results found in our study. Some studies show different results for some usability attributes. That was the case for learnability and also for ease of use for some authentication techniques.

Learnability

Table 21 shows the results for Learnability found in literature. In this case, one paper (Schaub, Walch, Könings, Weber; 2013) found that graphical authentication had a better learnability than in text based authentication. However, in another paper (Ma, Feng; 2011) it was found to be the opposite. Graphical authentication had a worst learnability than text based authentication. This in part because graphical authentication is a fairly new technology and people are not used to use it, making it harder to learn. The study that concluded that graphical authentication has a better learnability than text based did so by doing extensive research and also by the development of graphical passwords schemes by implementing different existing graphical password schemes on one smartphone platform. The study that concluded that graphical password have a worst learnability did so by conducting a longitudinal empirical study to examine the usability of traditional text password and graphical password, in a real life environment. The conflict of this could be by the difference of the studies in each of the papers, or the different people that did they did the studies on, the users.

Paper	Technique	Classification	Comparison	Other Technique
(Ma, Feng; 2011)	Graphical	Knowledge Based	worse than	Text based authentication
(Schaub, Walch, Könings, Weber; 2013)	Graphical	Knowledge Based	better than	Text based authentication

Table 21. Summary of authentication techniques comparison based on the learnability attributes according to research.

Learnability is summarized in table 22 below. In this case we used a positive symbol (+) to show the quantity of papers that say that one authentication method is better than the other, and the negative symbol (-) to show the opposite. For example, for graphical authentication one paper says it has a better learnability than text based while another paper says text based has a better learnability.

Learnability	
Graphical Authentication	Text Based Authentication
+ -	- +

Table 22. Conflicting Learnability Comparison

Ease of Use

Another attribute that was conflicted was ease of use (Table 23). In this case also with graphical authentication and text based authentication. In two papers graphical authentication was better than text based authentication. One of these conclusions (Ritter; 2013) was based on a new proposal for graphical authentication where they researched related work, the other one (Spitzer, Singh, Schweitzer; 2010) was based on a security project in graphical passwords where the goal of the project was to investigate a unique implementation of a graphical passwords scheme known as Cued Click Points. While in another paper (Ma, Feng; 2011) text based authentication was found to have a better ease of use. This last one was based on a longitudinal empirical study to examine the usability of traditional text password and graphical password, in a real life environment. The difference on this could also be because of the difference of the studies on the three papers.

Paper	Technique	Classification	Comparison	Other Technique
(Ma, Feng; 2011)	Graphical	Knowledge Based	worse than	text based
(Ritter; 2013)	Graphical	Knowledge Based	better than	text based
(Spitzer, Singh, Schweitzer; 2010)	Graphical	Knowledge Based	better than	text based

Table 23. Summary of authentication techniques comparison based on conflicting ease of use attributes according to research.

Table 24 below shows a summary of the conflicting ease of use attribute and the authentication techniques. The positive symbol (+) shows the quantity of papers that conclude that one authentication method is better than the other. The negative symbol (-) shows the opposite.

Ease of Use	
Graphical Authentication	Text Based Authentication
+ + -	- - +

Table 24. Conflicting Ease of Use Comparison

3.5.3 Lacking usability

On table 25 we can see the ISO/IEC 25010 (SQuaRE) quality model division for operability and usability with its attributes. The attributes in bold are the ones that were searched and we found results. The ones that have a light grey background are the ones that were searched and did not get any results. And the ones with a dark grey background are the ones that were not part of our research.

As shown in table 25, there were two attributes that were included in our search string for this research that were not found at all in the papers and those were ‘Attractiveness’ and ‘Appropriateness Recognisability’. Some papers referred to ‘willingness to use’ which may seem similar to ‘Attractiveness’. However the definition of Attractiveness based on the ISO/IEC 25010 (SQuaRE) is “the degree to which the product is attractive to the user” and we decided it not to use it as ‘Attractiveness’ since being attractive does not necessarily mean that the user is willing to use it.

The attributes not used in this research (see Table 25 dark grey background) are: Technical accessibility, Operability Compliance, Effectiveness, and Usability Compliance. Technical accessibility is defined as the degree to which users with specified disabilities can operate the product. This study does not take into account this attribute since it would require more emphasis on the different type of disabilities and how authentication techniques differ for each of them. Even though this was not included in our work we feel that this is an interesting topic that could be developed in the future.

Operability and usability compliance were left out of this study since it would require studies on many standards, regulations in law, style guides and conventions; which is out of our scope for this research. Effectiveness is defined as the accuracy and completeness with which users achieve specified goals. For this project we are focused on authentication techniques. Therefor we assume that all authentication techniques work well, that is, they all serve their porpoise of authenticating the user. A more detailed study about the effectiveness of the different authentication techniques would be out of our usability scope.

Characteristic	Atributes	Sub-atributes
Software Product Quality Model		
Operability	Appropriateness recognisability	
	Learnability	
	Ease of use	
	Attractiveness	
	Technical accessibility	
	Operability compliance	
System Quality-in-Use Model		
Usability	Effectiveness	
	Efficiency	
	Satisfaction	Likability
		Pleasure
		Comfort
		Trust
	Usability compliance	

Table 25. SQuaRE, 250100: Quality model division for operability and usability.

As we can see in Table 3 from chapter 2.4, there are many classifications and authentications techniques that were not discussed or studied relating their usability attributes. Especially for biometrics since the following techniques were not studied in terms of usability attributes: DNA Analysis, Facial Thermogram, Palm Print, Body Oder, Finger-knuckle-print, Hand Geometry, Ear Shape, Lip Shape, Gait.

As for the Computer/Smartphone classification none of the authentication techniques under that classification (Table 3) were analyzed in terms of their usability attributes. Those techniques are: Retrieve Password Stored on Device, Retrieve another secret from Device, SMS One time passwords, Device Generated One Time Passwords, and Out of Band Authentication (Phone Calls).

On table 26 we can see each the usability attributes studied for the authentication techniques and on table 27 we can see what classifications where studied in terms of their usability attributes. As you can see in table 28 it shows which authentication techniques were not studied at all in terms of their usability attributes.

Classification	Usability Attribute	Authentication Technique
Biometrics	ease of use	Face Recognition
		Fingerprint
		Hand Geometry
		Iris
		Keystroke
		Vein
		Voice
	satisfaction	Fingerprint
		Vein
Knowledge Based	ease of use	Graphical
		Password
		Pattern
		PIN
		Text based
	efficiency	Graphical
		Text based
	learnability	Graphical
		Text based
	memorability	Graphical
		Text based
	satisfaction	Graphical
		PIN
		Text based
Token Based	ease of use	Card

Table 26. Techniques and attributes studied.

Usability Attribute	Classifications
ease of use	Knowledge Based
	Token Based
	Behavioral
	Static
memorability	Biometrics
	Knowledge Based
	Token Based

Table 27. Usability attributes studied for the Classification of authentication techniques

Classification	Sub-Classification	Authentication Technique
Biometrics-based	Static/Physiological	DNA Analysis
		Facial Thermogram
		Palm Print
		Body Odor
		Finger-knuckle-print (FKP)
		Hand Geometry
		Ear Shape
		Lip Shape
	Dynamic/Behavioral	Gait
Token Based	Hardware Tokens	Key
	Computer/Smartphone	Retrieve Password Stored on Device
		Retrieve another secret from Device
		SMS One time passwords
		Device Generated One Time Passwords
		Out of Band Authentication (Phone Calls)

Table 28. Authentication Techniques not studied.

Some of these studies were based on a research of related work, others were based on projects from the authors where they investigated or implemented different authentication techniques to test their hypothesis, while others were based on longitudinal empirical studies to examine the usability of different authentication techniques. Since we used some of the most important electronic data sources to which we had access we will consider all of these studies as valid.

Considering the big amount of techniques that have not yet been studied in terms of usability attributes it lets us know that we still have a far way to go in terms of usability studies. Even if those techniques were studied there is a vast empty space on most of the

usability attributes, especially on attractiveness since we could not find even one paper that refers to it. Even though lately there has been more emphasis on usability there is still much more to research in terms of authentication. This shows that this field has not yet been fully studied.

3.6 Threats to Validity

Some of these papers use different studies for their analysis and conclusions. Some conducted surveys, others created their own applications to test out how the usability of those applications was. Our research is based on those studies which may be different from author to author.

Until we find other systematic reviews focusing in the usability attributes of authentication techniques we will not be able to validate our study externally.

As for internal validity, the three authors of this research were involved in this systematic mapping study. We discussed and agreed on the procedure and considered activities to counteract the effect of researcher bias. On the search string we used general terms and placed no constraints, in order to better achieve coverage and high accuracy.

The chosen time-frame was intended to include the last decade of research. We also selected some of the most important electronic data sources to which we had access, and added other external sources.

We were particularly careful during the exclusion process, not to discard any potentially interesting paper. For this reason, we also included papers whose abstract or title was not completely clear with respect to our research question for further reading.

4. CONCLUSION

With this research we have found many authentication techniques and were able to classify them into three different groups: Biometrics, Token Based, and Knowledge Based. Each of them with different sub-classifications and groups. While doing this research I encountered different authentication techniques that I was not familiar with. I was fascinated by how many Biometrics-based authentication techniques are, and in some cases I did not even know they were possible to do such as finger-knuckle-print (FKP), body odor, and gait.

While doing the classification of the authentication techniques I found interesting that many of the authors referred to the same thing, yet called it with a different name. This showed how a standard for these categories was needed. With these classifications it will be easier for people to understand under what classification certain techniques fall under. There are many techniques that are not yet widely use and little research material can be found on them.

There are new authentication techniques being proposed every year. As new techniques come along new classifications may appear and our table would need to be updated with those new techniques. For future work for the classification part of this project there would need to be a verification of new emerging techniques in order to know where to classify them or if a new classification would need to be proposed.

For the second part of our research we focused on the usability attributes based on the usability definition of ISO/IEC 25010 (SQuaRE). When I first saw the amount of papers returned by the search string I was overwhelmed thinking that most of them would be related to our topic. However once we were done reviewing and analyzing the papers I was surprised about how few papers were actually related to our topic.

We found that although there are many papers based on usability of different authentication techniques, there are not many that cover the attributes of usability, but speak of usability in general terms. This left us with little information about most of the usability attributes. The attributes that had the more information were memorability and ease of use. Other attributes such as: efficiency, learnability, and satisfaction had very little information.

There was one attribute that was not found at all and that was ‘Attractiveness’. Some papers referred to ‘willingness to use’ which I was tempted to assimilate to ‘Attractiveness’ but since the definition of Attractiveness based on the ISO/IEC 25010 (SQuaRE) is “the degree to which the product is attractive to the user” I decided not to use it, since just because something is attractive to the user it doesn’t mean that they are willing to use it.

We also found that many of the papers focus on some authentication techniques, leaving others with very little or none information. Especially for the classification of Biometrics based authentication. Since this classification has many techniques and it is fairly new technology it was difficult to find information related to their usability attributes. Some of them were: DNA Analysis, Facial Thermogram, Palm Print, Body Odor, Finger-knuckle-print, Hand Geometry, Ear Shape, Lip Shape, and Gait.

As for the Computer/Smartphone classification we see that none of the authentication techniques under that classification were analyzed in terms of their usability attributes. Techniques such as: Retrieve Password Stored on Device, Retrieve another secret from Device, SMS One time passwords, Device Generated One Time Passwords, and Out of Band Authentication (Phone Calls).

We found that many of the literature in our research focused mainly on two authentication techniques: graphical authentication and text based authentication. Probably because these two authentication techniques are the most used ones as of today. Analyzing the papers we concluded that graphical based authentication has a better memorability, satisfaction, and ease of use, than text based authentication, but a worst efficiency.

Looking back we can see how there is still a lot of research to be done for most of the authentication techniques in terms of their usability attributes. Although there has been a great advances and studies on usability, not much has been focused on authentication and its usability attributes. This may be a sign that this is a field which has not yet been fully studied and has a lot of opportunities for new researches.

.

5.REFERENCES

(Focardi; 2005) Focardi, R., & Informatica, D. (2005). Static Analysis of Authentication, 109–132.

(M. Samuel; 2010) John, M. S. (2010). Enhancing security of Pass Points system using variable tolerance, *274*, 270–274.

(Mariusz, Piotr, Khalid; 2010) Rybnik, M., Panasiuk, P., & Saeed, K. (2009). User Authentication with Keystroke Dynamics Using Fixed Text. *2009 International Conference on Biometrics and Kansei Engineering*, 70–75. doi:10.1109/ICBAKE.2009.42

(Maple, Schetinin; 2006) Maple, C., & Schetinin, V. (2006). Using a Bayesian averaging model for estimating the reliability of decisions in multimodal biometrics. *First International Conference on Availability, Reliability and Security (ARES'06)*, 7 pp.–935. doi:10.1109/ARES.2006.141

(Saxena; 2008) Saxena, A. (2008). Dynamic Authentication : Need than a Choice.

(Nosseir,Connor, Revie, Terzis; 2006) Nosseir, A., Connor, R., Revie, C., & Terzis, S. (2006). Question-Based Authentication Using Context Data, (October).

(Pusara, Brodley; 2004) Pusara, M., & Brodley, C. E. (2004). User re-authentication via mouse movements. *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04*, 1. doi:10.1145/1029208.1029210

(Manabe, Fukumoto; 2007) Manabe, H., & Fukumoto, M. (2007). AwareLESS Authentication : Insensible Input Based Authentication, 2561–2566.

(Asha, Chellappan; 2008) Asha, S., & Chellappan, C. (2008). Authentication of e-learners using multimodal biometric technology. *2008 International Symposium on Biometrics and Security Technologies*, 1–6. doi:10.1109/ISBAST.2008.4547640

(Bhattacharyya, Ranjan, Farkhod, Choi; 2009) Bhattacharyya, D., Ranjan, R., A, F. A., & Choi, M. (2009). Biometric Authentication : A Review, *2*(3), 13–28.

(Patil, Shimpi; 2013) Patil, K. I., & Shimpi, J. (2013). A Graphical Password using Token , Biometric , Knowledge Based Authentication System for Mobile Devices, (4), 155–157.

(NIST; 2011) Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., & Polk, W. T. (2011). NIST Electronic Guideline, (December 2011).

(Hiltgen, Kramp,Weigold; 2006) Hiltgen, a., Kramp, T., & Weigold, T. (2006). Secure Internet banking authentication. *IEEE Security & Privacy Magazine*, *4*(2), 21–29. doi:10.1109/MSP.2006.50

(Sethi, Manzoor, Sethi; 2012) Sethi, A., Manager, T., Manzoor, O., Consultant, S. S., Sethi, T., & Consultant, S. S. (2012 User Authentication on Mobile Devices.

(Witte, Rathgeb, Busch; 2013) Witte, H., Rathgeb, C., & Busch, C. (2013). Context-Aware Mobile Biometric Authentication based on Support Vector Machines. 2013 Fourth International Conference on Emerging Security Technologies, 29–32. doi:10.1109/EST.2013.38

(Bhattacharyya, Ranjan, Das, Kim, Bandyopadhyay, Kumar; 2009) *Bhattacharyya, D., Ranjan, R., Das, P., Kim, T., & Bandyopadhyay, S. K. (2009). Biometric Authentication Techniques and its Future Possibilities. 2009 Second International Conference on Computer and Electrical Engineering, 652–655. doi:10.1109/ICCEE.2009.103*

(Ma, Feng; 2011) Ma, Y., & Feng, J. (2011). Evaluating Usability of Three Authentication Methods in Web-Based Application. *2011 Ninth International Conference on Software Engineering Research, Management and Applications*, 81–88. doi:10.1109/SERA.2011.18

(Helkala; 2012) Helkala, K. (2012). Disabilities and Authentication Methods: Usability and Security. *2012 Seventh International Conference on Availability, Reliability and Security*, 327–334. doi:10.1109/ARES.2012.19

(Hamilton, Carlisle, Hamilton; 2007) Hamilton, S. S., Carlisle, M. C., & Jr, J. A. H. (2007). A Global Look At Authentication system muowstt gooderoguseu, (June).

(El-Abed, Giot, Hemery, Rosenberger; 2010) El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 170–178. doi:10.1109/CCST.2010.5678678

Tari, Ozok, Holden; 2006) Tari, F., Ozok, a. A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*, 56. doi:10.1145/1143120.1143128

(Forget, Chiasson, Biddle; 2010) Forget, A., Chiasson, S., & Biddle, R. (2010). Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. *Proceedings of the 28th international conference on Human factors in computing systems* - CHI '10, 1107. doi:10.1145/1753326.1753491

(Group M. I.; 2010) Group, M. I. (2010). Towards Understanding ATM Security – A Field Study of Real World ATM Use.

(Kataria, Adhyaru, Sharma, Zaveri, 2013) Kataria, A. N., Adhyaru, D. M., Sharma, A. K., & Zaveri, T. H. (2013a). A survey of automated biometric authentication techniques. *2013 Nirma University International Conference on Engineering (NUiCONE)*, 1–6. doi:10.1109/NUiCONE.2013.6780190

(Luca; 2008) Luca, A. De. (2008). EyePass - Eye-Stroke Authentication for Public Terminals, 3003–3008.

(Bauer, Cranor, Reiter, Vaniea ; 2007) Bauer, L., & Reiter, M. K. (2007). Lessons Learned From the Deployment of a Smartphone-Based Access-Control System, 64–75.

(Riley, Mccracken, Buckner; 2007) Riley, C., Mccracken, H., & Buckner, K. (2007). Fingers, Veins and the Grey Pound : Accessibility of Biometric Technology, (August), 28–31.

(Ritter; 2013) Ritter, D. (2013). MIBA : Multitouch Image-Based Authentication on Smartphones, 787–792.

(Schaub, Walch, Könings, Weber; 2013) Schaub, F., Walch, M., Könings, B., & Weber, M. (2013). Exploring the design space of graphical passwords on smartphones. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. doi:10.1145/2501604.2501615

(Schlöglhofer, Sametinger; 2012) Schlöglhofer, R., & Sametinger, J. (2012). Secure and usable authentication on mobile devices. *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM* '12, 257. doi:10.1145/2428955.2429004

(Spitzer, Singh, Schweitzer; 2010) Spitzer, J., Singh, C., & Schweitzer, D. (n.d.). A security class project in graphical doi:10.1109/ICCEE.2009.103

(Braz, Robert ; 2006) Braz, C., & Robert, J. (2006). Security and Usability : The Case of the User Authentication Methods, 199–203.

(Trewin, Swart, Koved, Martino, Singh, Ben-david; 2012) Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-david, S. (2012). Biometric Authentication on a Mobile Device : A Study of User Effort , Error and Task Disruption, 159–168.

(Wright, Patrick, Biddle; 2012) Wright, N., Patrick, A. S., & Biddle, R. (2012). Do You See Your Password? Applying Recognition to Textual Passwords.

(Zezschwitz, Dunphy, Luca; 2013) Zezschwitz, E. Von, Dunphy, P., & Luca, A. De. (2013). Patterns in the Wild : A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices, 261–270.

(ISO/IEC; 2011) ISO/IEC, 2011, ISO/IEC 25010, Software Product Quality Requirements and Evaluation (SQuaRE) – Quality Models for Software Product Quality and System Quality in use. International Standard. Switzerland.

(Cysneiros, Kushniruk; 2003) Cysneiros, L. M., & Kushniruk, A. (2003). Bringing Usability to the Early Stages of Software Development Usability Ontology References.

(Khan, Sulaiman, Said, Tahir; 2011) Khan, M., Sulaiman, S., Said, A. M., & Tahir, M. (2011). Usability studies in haptic systems. *2011 International Conference on Information and Communication Technologies*, 1–5. doi:10.1109/ICICT.2011.5983569

(Ramil, Jaafar; 2008) Ramli, R. B. M., & Jaafar, A. B. (2008). e-RUE : A cheap possible solution for usability evaluation. *2008 International Symposium on Information Technology*, 1–5. doi:10.1109/ITSIM.2008.4632048

APPENDIX

Appendix A

Definitions:

Biometric Based : Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits . It is based on “Something You Are”. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users. (Patil; Shimpi; 2013)

Token Based: It is based on “Something You Possess”. For example Smart Cards, a driver’s license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. (Patil; Shimpi; 2013)

Knowledge Based Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge-based authentication (KBA) is based on “Something You Know” to identify you For Example a Personal Identification Number (PIN), password or pass phrase. (Patil; Shimpi; 2013)

Static/Physiological: Physiological systems of identification deal with statistical characteristics of a person: fingerprints, iris recognition, hand geometry, DNA, face recognition, palm print. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Dynamic/Behavioral : Behavior methods of identification pay attention to the actions of a person, giving the user an opportunity to control his actions. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Image Based: user is given a pool of images and the user has to re cognize and identify the images, which he or she selected during the time of registration.In recall based techniques, the user has to reproduce something he or she created at the time of registration. (M. Samuel; 2010)

Fingerprint: A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Fingerprints are the most commonly used biometrics solution as they are less expensive compared with other biometrics solutions. Fingerprints can be used for authenticating students’ submissions of e-exams via the use of low cost biometrics devices. Fingerprints can be scanned, transmitted and matched with the aid of a simple device. (Asha, Chellappan; 2008)

DNA Analysis: DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Palm Print: Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical readers that are very similar to those used for fingerprint scanning, their size is, however, much bigger and this is a limiting factor for the use in workstations or mobile devices (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Hand Geometry: It is based on the fact that nearly every person's hand is shaped differently and that theshape of a person's hand does not change after certain age. These techniques include the estimation of length, width, thickness and surface area of the hand. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Face Recognition: an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is the most natural means of biometric identification (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Body Odor: The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to obtain the odor from nonintrusiveparts of the body such as the back of the hand. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Ear Shape: Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Optophone) is produced by a French company ART Techniques. It is a telephone type handset within which is a lighting unit and cameras which capture two images of the ear (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Retina Scanning: It is based on the blood vessel pattern in the retina of the eye as the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Facial Thermogram: Thermographic cameras detect radiation in the infrared range of the electromagnetic spectrum and produce images of that radiation, called thermograms. Since infrared radiation is emitted by all objects above absolute zero according to the black body radiation law, thermography makes it possible to see one's environment with or without visible illumination. (Kataria, Adhyaru , Sharma, Zaveri; 2013)

Iris: This recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through video based image acquisition system. Each iris structure is featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings

Keystroke dynamics: Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur

two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the Biometric Systems 32 typist. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Gait: Gait is the pattern of movement of the limbs of animals, including humans, during locomotion over a solid substrate. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or major injuries involving joints or brain. (Kataria, Adhyaru, Sharma, Zaveri; 2013)

Voice: Voice is also physiological trait because every person has different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral. (Bhattacharyya, Ranjan, Farkhod, Choi; 2009)

Retrieve Password Stored on Device: This is an approach that applications often use; they will ask the user to enter his/her password the first time the application is started, and will store it on the device for subsequent authentication (either in the clear, or encrypted using a key stored on the device). (Sethi; Manzoor; Sethi; 2012)

Retrieve another secret from Device: instead of storing the password on the device, another secret is stored on the device by the application. The secret can be a random ID, a cryptographic key, the user's password encrypted using a key stored only by the server, etc. (Sethi; Manzoor; Sethi; 2012)

SMS One time passwords: This authentication scheme leverages short messaging service (SMS) to deliver a one-time-password (OTP) to a configured device. (Sethi; Manzoor; Sethi; 2012)

Device Generated One Time Passwords: These are One-Time-Passwords (OTPs) generated by software running on a mobile device. A software token application on the device is responsible for generating OTPs that the user can use to authenticate to an application. (Sethi; Manzoor; Sethi; 2012)

Out of Band Authentication (Phone Calls): uses a separate channel from the one that is being used for general communication to authenticate a device. When a user attempts an operation that requires out-of-band authentication, the server automatically calls the user's registered mobile phone. The user answers the phone and authenticates using some factors (PIN/password, OTP, and/or voice biometrics). (Sethi; Manzoor; Sethi; 2012)