



POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

Toward a usable system-generated authentication mechanism

Relatori

Prof. Antonio Lioy
Ing. Andrea Atzeni

Candidato

Federica SARTI

ANNO ACCADEMICO 2019-2020

*Ai miei genitori,
alla mia famiglia
e ai miei amici più cari.*

Summary

The objective of this thesis is to investigate through objective metrics the usability of a new system-generated authentication mechanism, based on the concept of implicit memory, with the purpose to overcome the unreliable subjective human component in both authentication and usability evaluation.

The first part of this work aims to analyse the state of the art of authentication systems, presenting their advantages, disadvantages and usability issues.

Particular attention is given to system-generated authentication mechanisms, which permits to address the human related vulnerabilities (e.g. predictability) and to provide a greater degree of security.

In this context, novel system-generated authentication mechanisms, based on the concept of implicit memory, are examined. These systems exploit the ability of the human brain to acquire and store information unconsciously, resulting in the complete abolition of the cognitive effort derived from recall of information from memory and therefore addressing the representative problem of memorization of the system-generated systems.

The second part of the thesis focusses on the examination of usability evaluation methods, with specific interest for the objective metrics, in particular concerning user satisfaction. In this regard, emerging physiological objective metrics are presented, such as eye-tracking, heart rate variability (HRV) or electromyography (EMG).

The intent of introducing this new category of metrics is to obtain unbiased assessments, which are not subject to human brain reprocessing of lived experiences.

Although for the usability components of efficiency and effectiveness various analytical data can be gathered, in reference to satisfaction, self-report questionnaires are predominantly exploited. Notwithstanding the importance of questionnaires to obtain information from the target audience, as a matter of fact, humans represent an unreliable element, affected by several response biases, which compromise the entire evaluation.

The final part of the thesis describes the prototype implementation, the usability test realization and the results achieved.

The prototype is a graphical authentication system, which exploits the visual-motor skills unconsciously learned by the user, in accordance with the implicit memory concept. Indeed, the user does not have to make any cognitive effort neither for the creation nor for the memorisation of the secret, which is uniquely associated by the system to the individual and it must not be remembered.

The test has the purpose to evaluate the usability of the prototype, with a selection of objective metrics. The metrics include a series of data directly obtained by the log file, such as time and the number of failures during the completion of tasks, and information collected by eye and mouse tracking heat-maps, in addition to the heart rate variability data, collected by means of a bracelet with optical heart rate sensor.

As a matter of fact, although these new approaches permit to gather reliable data concerning the emotional state of the user, they do not provide any information regarding the positivity or negativity of the emotion experienced. Consequently, in order to evaluate and compare the information obtained through these new metrics, subjective questionnaires were inserted concerning the emotional state of the user.

A total of 22 participants has been tested, with heterogeneous experiences in the utilisation of IT systems. A primary interesting result concerns the positive first impression of the system among the participants, although they had never experienced anything similar. In fact, over one half of the participants agreed with the idea of replacing their traditional authentication methods with the proposed one, especially for the absence of cognitive effort by the user, who must not memorise or recall any kind of information. This outcome is impressive, because it reveals users' awareness of the inadequacy of username/password mechanisms and the will to migrate towards something more innovative.

Acknowledgements

The work described in this monograph was conducted under the supervision of Prof. Antonio Lioy and Ing. Andrea Atzeni, who supported me in every step of this work, with immense patience and wisdom.

Contents

1	Introduction	10
2	Background	13
2.1	User authentication	13
2.2	Knowledge-based authentication	14
2.2.1	Alphanumeric passwords	14
2.2.2	KBA challenge-response	17
2.2.3	Graphical passwords	18
2.3	Ownership-based authentication	23
2.3.1	Disconnected token	24
2.3.2	Connected tokens	25
2.3.3	Contactless tokens	27
2.3.4	Mobile phone tokens	29
2.4	Inherent-based authentication	30
2.4.1	Physical biometric authentication	31
2.4.2	Behavioural biometric authentication	37
2.5	Conclusion	43
3	System-generated secrets	44
3.1	User-chosen and system-assigned secrets	44
3.1.1	System-generated passwords	45
3.2	Enhancements to improve memorability of system-assigned secrets	46
3.2.1	Pronounceable passwords	46
3.2.2	Chunking	46
3.2.3	Method of loci	47
3.2.4	Link method	47
3.2.5	Exploitation of implicit memory	49
3.3	Conclusion	53

4 Usability evaluation	54
4.1 Usability definitions	54
4.2 Background	56
4.2.1 Usability evaluation	56
4.3 Evaluation location	62
4.3.1 Conclusion	64
4.4 Usability measurement	64
4.4.1 Context analysis	64
4.4.2 Usability metrics	67
4.5 Usability evaluation of authentication methods	77
4.5.1 Alphanumeric passwords	78
4.5.2 Graphical passwords	79
4.5.3 Token	81
4.5.4 Biometric authentication	81
4.6 Conclusion	83
5 Usage scenarios	84
5.1 #1: Company profile	84
5.2 #2: Secrets Management	87
5.3 #3: Online payment	89
5.4 #4: ATM withdrawal	91
5.5 #5: PC unlock	94
5.5.1 Local user account	94
5.5.2 Domain account	96
6 Usability test	98
6.1 Prototype test	98
6.2 Usability evaluation structure	100
6.3 Implementation	101
6.3.1 Prototype	102
6.3.2 Usability evaluation	102
7 Results Analysis	105
7.1 Context	105
7.2 Registration	105
7.3 Training	106
7.4 Login	108
7.5 Final questionnaire	110
7.6 OGAMA test	114

8 Conclusion and future work	118
A User manual	120
A.1 The system	120
A.2 Test execution	120
A.3 Homepage	121
A.4 Registration	121
A.5 Training	121
A.6 Login	122
A.7 Personal page and secondary operations	122
A.7.1 Book your trip on the minibus	123
A.7.2 Delete your trip	123
A.7.3 Change username	123
A.7.4 Delete account	123
A.8 Logout	123
A.9 Installation manual	124
A.9.1 Web server	124
A.9.2 Database	124
B Programmer manual	129
B.1 Development environment	129
B.2 Global variables	129
B.2.1 Dimensions	130
B.3 Folders	130
B.4 Server side	130
B.5 Client side	134
Bibliography	139

Chapter 1

Introduction

One of the most significant parts of any system is authentication. Indeed, the majority of the challenges in Internet security can be related to authentication. As a matter of fact, it represents the first and the last line of defence in a great portion of systems, avoiding unauthorized accessing to users' confidential data [8].

The technological advancements of the last decades allowed the spread of technologies worldwide, resulting in the utilisation of multiple devices by the majority of the global population, both for personal and business use. In this context, the issue of granting the access uniquely to authorized individuals has become increasingly incisive, considering the continuous improvements of the attacks, constantly more specific.

Heretofore, unfortunately, the mechanisms provided rely on the human component, which is strongly unreliable and undermines the security of systems itself. In fact, it is typically required to the user to create secrets and subsequently handle the entire management procedure, which include memorisation and maintenance of confidentiality.

However, humans tend to invent based on their experiences, their memories, their affections and even in case of remarkably inventive capabilities, which allow not to include personal matters, they are guided by an unconscious preference for symmetry, which causes conventional schemes, such as the insertion of numbers in the center of a sequence of letters (e.g. "kfg503lLa"). As a result, anything produced by the human brain occur to be extremely predictable.

Furthermore, the necessity to minimise the vulnerabilities and the risks of attacks led to extremely complex requirements imposed to the users, who exhibit evident difficulties in satisfying the constraints. As a consequence, particularly unsecure behaviours, such as reuse, have become typical.

In addition to the aforementioned issues, which derive by the consistently prioritisation of security over usability by the designers of the systems, further secrecy problems arise from the human inability to keep private the secrets. Together with the improper behaviour of writing down, whenever it is possible, the advent and the increasing use of social media and similar types of platforms, induces users to spontaneously and even unconsciously publish personal information. In this manner, sensitive data generally exploited in the creation of secrets (e.g. photos or important dates) are made available to a potentially global audience, which include malicious attackers.

For example, information gathering about the victims throughout their profiles permits to an attacker to learn about the answers used to change the password (e.g. the name of the pet or the primary school teacher). A recent example is mentioned in the article "FBI warning: Cyberthieves mining social media for personal data to hack accounts" in the Pittsburgh Post-Gazette by Torsten Ove [144], in which it is stated: "Eugene Kowel, acting special agent in charge of the Pittsburgh FBI, warned about revealing information such as where you went to high school, the school mascot or your first pet because criminals can gather that information and use it to pose as you and reset your passwords."

The drastic drop in the usability of the authentication mechanisms, concern not only the creation and maintenance of secrets, but also the tedium generated by the double authentication

methods, which forces users to bring an additional mandatory object (e.g. token or smartphone), or even the difficulty of accepting the biometrics methods, frequently considered invasive and often fallacious.

The mentioned problems have induced researchers to develop something new, which eliminates the predictable behaviour of humans and restore the security of authentication systems to an adequate level. These novel mechanisms automatically generate complex but robust secrets to be provided to the users.

The major flaw regarding the memorability of the secrets produced is generally solved with the implementation of automatic password saving mechanisms, known as “password managers”. For example, the Google password manager permits to view, change or remove passwords saved in the Google Account.

Although these mechanisms are widely exploited, they represent a palliative.

In order to completely exclude the human component from the authentication systems, the memorisation problem must be eradicated.

Although several techniques have been formulated to better memorise any type of information, it must be considered the precariousness of human memory, which is extremely unreliable, and the fact that they are not adopted by the majority of the people.

In this regard, new studies have been done on the implicit memory of humans and how it can be included in new authentication methods.

The implicit memory mechanism, associated with a system-generated approach, allows to eliminate the failure of the human component from the authentication. In fact, the creation is entrusted to the system, while the human brain’s ability to acquire information without being truly aware is exploited for memorization.

The combination of these techniques permits to develop new authentication methods that can finally supplant the vulnerable and tedious dominance of passwords.

Notwithstanding it is notorious that security and usability represent opposite directions to be carefully equilibrated in a system, researchers have consistently prioritized security over usability. Indeed, usability has recently become a central theme in security, since the success or failure of a system relies on the perception that users have of it.

In fact, however innovative and secure a mechanism may be, if it is not considered usable, it will not be successful.

As a consequence, it is essential from the point of view of the evaluation of the usability of a system, that bias of any kind do not influence the results. However, when a usability test is performed, it is inevitable to encounter bias introduced by humans, which contaminate the outcomes.

Although some usability characteristics, such as effectiveness or efficiency, are based on analytical data obtained from user interaction with the system, satisfaction (i.e. further fundamental usability component) relies, instead, only on the user subjectiveness. In fact, in the majority of cases, satisfaction is tested through self-report questionnaires, where the user have to answer a series of questions in the most sincere way possible.

Nevertheless, there are known biases in this approach, such as those grouped under the name of *response bias*¹, including the *acquiescence bias* (i.e the tendency to agree with the question proposed) or the *extreme responding bias* (i.e. the tendency to select the most extreme responses available), that affect the results of the test.

Flaws in the self-report evaluation methods can be observed decades ago. For example, in 1994, Jakob Nielsen was already briefing on this problem [156]:

¹“Response bias is a general term for a wide range of tendencies for participants to respond inaccurately or falsely to questions. These biases are prevalent in research involving participant self-report, such as structured interviews or surveys. Response biases can have a large impact on the validity of questionnaires or surveys.” from https://en.wikipedia.org/wiki/Response_bias

“To design the best UX, pay attention to what users do, not what they say. Self-reported claims are unreliable, as are user speculations about future behaviour. Users do not know what they want.”

The reason is that in reporting something to be recalled from memory, people rationalize their behaviour. Consequently, a large number of reasons can be specified for questionnaires to not be entirely valid, including the impression of self that the participant wants to give and therefore honesty of the responses, and the possible deficiency regarding the introspective ability to provide an accurate response to a question [157].

Considering that usability is strongly affected by human factors, which compromises the evaluation of the system, it gained importance the necessity to evaluate users' performance in an objective manner, since according to Jakob Nielsen [158]:

“Inadequate use of usability engineering methods in software development projects have been estimated to cost the US economy about \$30 billion per year in lost productivity.”

Chapter 2

Background

In this chapter, the state of the art of authentication mechanisms is presented, observing the subdivision into factors of knowledge, possession or inheritance.

Different best-known authentication systems will be introduced, with particular interest in their strengths, weaknesses and usability issues.

2.1 User authentication

At present times, user authentication is a process embedded in almost every system, in an enormous amount of variations. Indeed, the objective of authentication is to ensure that only specific authorized users can access confidential data for the specific application utilised.

Throughout the past years, numerous authentication mechanisms with different strengths and weaknesses have been proposed and deployed depending on the context of use [2, 5]. They can be broadly classified into three main categories:

1. Knowledge-based authentication mechanisms (“*what you know*”);
2. Ownership-based authentication mechanisms (“*what you have*”);
3. Inherent-based authentication mechanisms (“*what you are*”).

Different types of the aforementioned authentication methods can be combined to increase security and provide the so called multi-factor authentication, depending on complexity, costs and the level required by the application within which it will be implemented [4].

The following table briefly summarizes the strengths and weaknesses of the previously mentioned authentication schemes.

AUTHENTICATION METHODS	WEAKNESS	STRENGTH
Knowledge-based	Recall-memory strain, vulnerable to security attacks including collusion, guessing, lost credentials, dictionary attacks and brute-force attacks	Easy to use, cost effective and very popular
Ownership-based	Objects can be shared or lost, additional cost required as it uses special input device, deployability to other platforms is not easy	Resist adversaries’ attacks, no recall
Inherent-based	Additional cost used for input device, False Accept Rate, False Reject Rate, Equal Error Rate, Failure to Enrol Rate and Failure to Capture Rate, not compatible with other platforms.	No recall , nothing to carry, most reliable

Table 2.1: Strengths and weaknesses of typical authentication schemes [6]

2.2 Knowledge-based authentication

Knowledge-based authentication mechanisms lay their foundations on a memorized secret that only the user knows, which can be:

- an alphanumeric password, with the particular case of Personal Identification Number (PIN);
- a response to specific questions;
- a graphical secret.

Although the vulnerabilities of knowledge-based authentication schemes are notorious, they -and more specifically passwords- remain currently the most common approaches for authentication, since, in many instances, they are considered the best-fit solutions. Indeed, compared to the other two mechanisms, they do not entail high development and administrative costs, they are portable, they do not have specific security flaws as in tokens (e.g., loss or theft) and in biometrics (e.g. fingerprints extracted from touched objects) and they do not have privacy issues of biometrics.

On the other hand, according to Christina Katsini et al. [2], knowledge-based authentication presents security as a contract between the provider, which imposes the terms, and the user, who has to conform to them with no way to reply. It is evident that this practice raises usability issues, imputable to the continuous-increasing memorising requirements which induce users to reuse and write-down secrets [4].

In the following sections the three main knowledge-based techniques will be explained in more detail.

2.2.1 Alphanumeric passwords

Alphanumeric passwords are the original knowledge-based authentication mechanism since the beginning of authentication history back in the 60s. Thenceforth, even though it has been proven that they are the most vulnerable security system, passwords remain the most popular and yet unavoidable method, owing to their many advantages, such as the convenience of use and the simple implementation [6].

In the general scheme, the claimant has to prove to know the secret, which can be either a password or a passphrase, and writing it in the specific provided field of the authentication page. Subsequently, it will be compared to the value stored in the verification table in the application database, in order to finalize the authentication and allow the access to the data.

The above cited secret must fulfil the requirements imposed in the registration phase, to ensure sufficient complexity and secrecy in order to be impractical for an attacker to guess or discover the correct secret value. Unfortunately, as a consequence, users frequently forget their keyword and tend to reuse already adequate ones. Therefore, it has become imperative to incorporate expensive customer supports or automated backup authentication schemes, which could include extremely weak mechanisms, such as backup questions [8].

In recent years, researchers have been attempting to resolve above-mentioned issues caused by human improper behaviours and concentrate on users' needs, in order to make the constraints imposed by the guidelines less severe. For example, in June 2017, the United States National Institute of Standards and Technology (NIST) issued a new revision of their digital authentication guidelines, NIST SP 800-63B-3 [159], stating that secrets must be at least 8 characters in length to a maximum of 64 and Unicode [ISO/ISC 10646] as well as all printing ASCII characters, including the space character, should be acceptable.

Nevertheless, the fault for human difficulty in managing passwords should not be entirely attributed to the straight requirements. Indeed, nowadays, the amount of passwords of the users' various accounts (e.g. email, bank, social media or work profiles) is significantly massive. Considering that each password should be unique, the cognitive effort required to the users, both for creation and memorisation, becomes seriously intense.

Notwithstanding the intent to move towards greater usability of these systems, it must be considered that the current restrictions derive from a series of vulnerabilities that characterise these mechanisms and therefore they are essential for the security of the systems.

In the following section the basic attacks that undermine the security of these mechanisms are presented.

Basic attacks

Attackers have developed an extensive number of techniques to stole users' passwords, such as Men-In-The-Middle (MITM), phishing or keylogging attacks [8].

Offensives can be partitioned in three main categories [5]:

1. technical (or brute force) attacks;
2. discovery attacks;
3. social engineering attacks.

Brute force attacks generally involves two different methods. The first consists in attempting passwords against the system, which could be easily resolved with a basic lockout; the second correspond to a violation of the password hash file, where the passwords are saved in the form of encrypted text. This exploit can be performed offline on a high speed PC, attempting millions of keys per second, in fact it corresponds to a processor-intensive search through the entire password keyspace, calculating and comparing hash values of potential passwords to the values in the stolen hash file.

In practical terms, brute force attacks can be very time consuming, since a password with n characters, where each of those can have c different values, will have a keyspace size of

$$k_p = c^n$$

and therefore high-performance computers are essential to explore it entirely in a feasible amount of time [4]. For this reason the first defence-line involve increasing keyspace through the use of salts¹, and include for example a physical protection to the password hash file. In addition, it is commendable to use combination of long words which cannot be found in common password dictionaries, in combination with mixed symbols (e.g. upper/lower characters and special symbols) and a periodic change of the password.

More sophisticated brute force attacks are *dictionary attack*, where only most-likely-to-succeed strings in a pre-arranged list are tried and *rainbow table attack*, where special pre-calculated database allow to reach a compromise between memory and calculation time.

Password discovery attacks include a varied range of means, ranging from interception, to the exploitation of several mechanisms or Trojan programs capturing keystrokes, or the discovery of default passwords. This is a targeted, directed, system-level exploit aimed at specific access, whether through another account to increase privilege or across systems for common users and accounts. In this category can be entered sniffing attacks, replay attacks and several others.

The primary defence against discovery are proper system design rules, which do not allow discovery of passwords through scripts or default system accounts.

Social Engineering consist in the attempt by an intruder to obtain password and account information from the user. This attack does not concern computer system, considering that phone, fax, email, or casual contacts are employed. Moreover, the attack is often disguised in a very

¹A *salt* is an additional random string of data used to modify a password, in order to prevent collisions even in the case two different users created the same identical password. For each password generated, the salt is concatenated to it and the entire string is processed with a cryptographic hash function, in order to be securely stored.

official sounding and persuasive manner. This method takes advantage of a person's willingness to help and indeed all requests are typically indirect and subtle enough that often the victim is not aware they are divulging information. The primary defence against this type of exploit is training and awareness directed at the users, with respect to this specific vulnerability.

In conclusion, password-based authentication represent a weakest technique, with a superficial resistance to attacks. It is subject to extremely unsecure behaviours of users, who tend to write them down or disclose them to third parties.

Since this is still the predominant authentication method, it is crucial for users to be aware and sincerely understand the possible attacks and the threats that an inappropriate utilization can cause.

PIN

A particular type of alphanumeric password is the Personal Identification Numbers (PIN), which correspond to a memorized secret generally composed of only decimal digits.

Developed in the beginning for systems whose input was mainly numeric (e.g. telephone systems or Automatic Teller Machines (ATMs)), nowadays its principal function concern operations that require quick and easy, but yet sufficiently secure access (e.g. electronic transactions or unlocking mobile devices).

Analogously to passwords, PINs are remarkably utilized despite their considerable number of deficiencies, including a reduced keyspace and memorability issues. These type of problems ensue from the human incapability to remember long sequences of numbers, forcing the length from 4 to not more than 9 ciphers. The result is that the keyspace could eventually be significant, providing a considerable improvement in security, but the entropy² will be marginal as users tends to prefer commonly selected PINs, such as calendar dates. As a consequence, some PIN selection policies have been imposed to assist users in the creation process, for example blacklist policy (e.g., forbidding the most popularly used PINs, such as 1234 or 0000), which facilitate the generation of both secure and memorable PINs [15].

Furthermore, they are exposed to several attacks, most of which in common with passwords, as brute force or keylogger attacks but also shoulder-surfing, screen dumping and permutation. More specific definitions are provided below:

Keylogger is a code installed by malware in a machine with a keyboard input, with the intent to monitor victim's activity and gather confidential information, such as credentials, in order to be successively used or sold. Nowadays, improved keylogger software with enhanced features have been developed, permitting to capture mouse activity, desktop activity and even deceive all major anti-virus and anti-spyware scanners.

Shoulder-surfing consists of a physical person standing behind the victim and observing the actions performed on the device, with the aim to apprehend sensitive information.

Screen dumping is the technique of taking a screenshot of the monitor from a compromise device, in order to obtain the victim's data, such as the login credentials.

Permutation permits to generate every possible permutation of the value inserted, which is easier to calculate in proportion to the length of the secret.

Over time, various attempts to overcome the PIN-entry mechanism vulnerabilities have been made by researchers with any consistent outcome.

For example, Roth et al. [4] created a PIN entry mechanism, which requires four key presses for each digit. Furthermore, eye-gaze interaction methods have been investigate by De Luca et. al [9], underlining the advantages equally in implementation and in the ease of use of this technique,

²Common metric used for the estimation of password strength. It refers to how randomly users select passwords from a given keyspace, decreasing the probability of guessability.

which consist in performing a specific eye movement pattern which triggers an action.

Unfortunately, although these systems are resistant to shoulder-surfing attacks, they do not provide protection against camera-based attacks. In this regard, indirect input mechanisms have been examined, but they arose problems concerning the addition of significant overhead to the input.

Further new techniques, such as ColorPIN [10], does not involve the user to protect the input. In fact the major security problem of PIN based authentication is that there is no security built into it and users have to actively take care of securing the input.

Currently, companies provide system-generated PINs constantly longer to strengthen PIN security, unconcerned about memorability challenges. Hence, research has been focusing on the resolution of this crucial issue, in particular Gutmann et al. [11] propose an alternative method of generating random PINs excluding automatic procedures, which involve the users demanding which memorisation strategy they prefer and release a PIN that matches it.

In conclusion, PINs are currently massively used but not alone, regularly with an additive authentication mechanism.

2.2.2 KBA challenge-response

Knowledge-Based Authentication schemes are challenge-response mechanisms, typically utilized as a component in multi-factor authentication or for password retrieval. In general the user is required to answer at least one question, whose response represent the shared secret.

KBA systems can be subdivided into two different schemes:

1. *static*, in which a set of questions and relative responses are previously selected by the user during the registration phase (e.g. “How many pets do you have?”, “What is your favourite food?” or “Who was your favourite teacher?”) (Fig. 2.1 and Fig. 2.2);
2. *dynamic*, in which questions are not agreed with the user at a preliminary stage, but formulated depending on gathered information from public records (e.g. “What was your street address when you were 10 years old?”) and response must be insert within a defined brief period of time in order to be considered correct, otherwise they expire (Fig. 2.3).

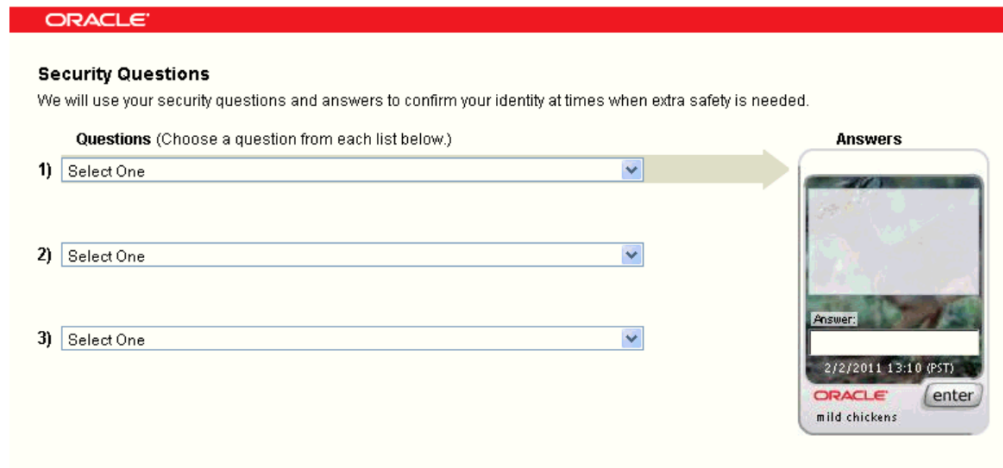
Dynamic KBA has been introduced, in order to resolve the guessing drawbacks of static KBA with pre-agreed personal challenge questions, which implied an extremely weak authentication mechanism. In order to overcome static KBA limitations, dynamic questions and answers are generated on-the-fly leveraging user’s activity logs, such as past financial activities, shopping behaviours, browsing history, emails and smartphone usage patterns. Several variants have been proposed, for example based on user’s browsing history in a recent period, electronic personal history such as calendar or email information, or even users’ geo-temporal history.

Nevertheless, the generation of challenging and diversified questions remains a pending matters.

A comprehensive description of a KBA challenge-response mechanism is described in a Oracle guide, “Managing Knowledge-Based Authentication” [139].

Examples of guessing vulnerabilities of this method are proposed in [26], where different studies have been analysed and results state that approximatively the 80% of the responses is remembered by participants and about the 40% of the time, attackers or friends and relatives were able to correctly guess the answers. Furthermore, it has been reported that participants were unable to recall around the 20% of their answers within three months.

Moreover, it is evident that a meticulous research on several online sources (e.g. social media or public records), allow anyone to find valuable information to exploit in an attack. In addition, the majority of the challenge questions are regularly reutilised across different websites, facilitating attackers in intruding into multiple accounts. The reason can be related to the fact that the questions must underlie common criteria, such as ease in remembering, adequacy for large part of the population, difficulty in guessing or discovering, and correspondence with a single answer.



ORACLE

Security Questions
We will use your security questions and answers to confirm your identity at times when extra safety is needed.

Questions (Choose a question from each list below.)

1)

2)

3)

Answers

2/2/2011 13:10 (PST)
ORACLE
mild chickens

Figure 2.1: KBA example from [139]



My Name

Gender

Birthday

I live in

Postal Code

2. Select an ID and passwo

Yahoo! ID and Email

Password

Re-type Password

3. In case you forget your ID

Alternate Email

1.Security Question

Your Answer

2.Security Question

Your Answer

Figure 2.2: KBA example from [145]

2.2.3 Graphical passwords

Graphical user authentication is the latest knowledge-based authentication technique presented as an alternative solution to the text-based authentication. These recent systems arise as a result of various psychology studies which reveal a human brain tendency of better remembering images rather than verbal or textual information. In fact, memorability is a major issue leading users in breaking basic security rules, such as using very simple passwords, writing them down or reuse[2].

Researchers distinguishes between three types of graphical password schemes, named after the way they strain the users' memory:

1. purely recall-based schemes;
2. cued-recall-based schemes;
3. recognition-based schemes.

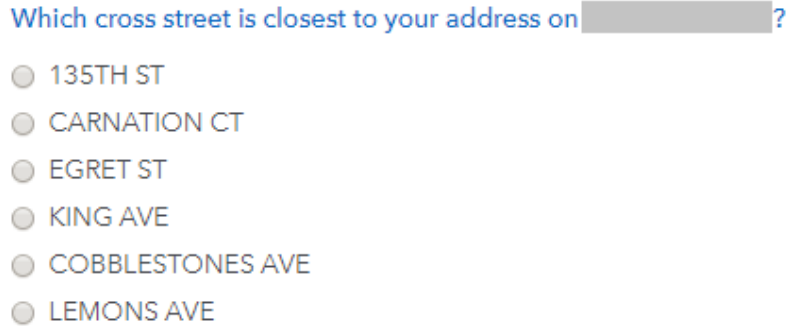


Figure 2.3: KBA example from [145]

In general, graphical password techniques have several drawbacks, such as limited authentication key pool compared to alphanumeric passwords, shoulder-surfing and image gallery attacks. Furthermore, it should be mentioned that all graphical password schemes have some inherent weaknesses concerning people with eyesight problems, poor motor control and people with various kinds of colour blindness, who may not be able to effectively exploit them [14]. In addition, it is important to consider that various studies suggest to use pictures with semantically meaningful content, because abstract images may be less memorable than concrete scenes. Indeed, long term memory stores a meaningful interpretation of the image that captures the sense of the image in preference to unimportant visual details. Moreover, graphical passwords exploit rehearsal or repetition in both registration and login processes in order to have the secret long-term-memorized, with the consequence of making them seriously time-expensive and even tedious for the users.

In the following sections the three categories are analysed in more detail.

Purely recall-based

Purely recall-based schemes are cognitive arduous systems on which also traditional textual password authentication are based. They request a considerable mental strain by users, who are supposed to exactly remember and reproduce the secret, with an actual limited range of attempts. Some examples of this type of graphical passwords are the draw-metric-based schemes (e.g. Android screen unlock or *Draw-A-Secret*) and the search-metric schemes (e.g. *grIDsure*) [12].

These approaches expect the user to draw the authentication secret using a stylus or a mouse to access the application, relying on the fact that it should be more memorable compared to passwords, since they combine visual, lexical and kinaesthetic memory.

Unfortunately, this represent the first cause of vulnerability considering that has been demonstrate that people tend to generally create symmetrical figures. Thereby the keyspace becomes evidently reduced, making guessability attacks extremely simple (i.e. brute-force and dictionary attacks) [13].

Moreover, these methods have been proven susceptible to other various attacks, including observability (i.e. shoulder-surfing and spyware) and recordability (i.e. Social Engineering) attacks, as well as memorability difficulties [12].

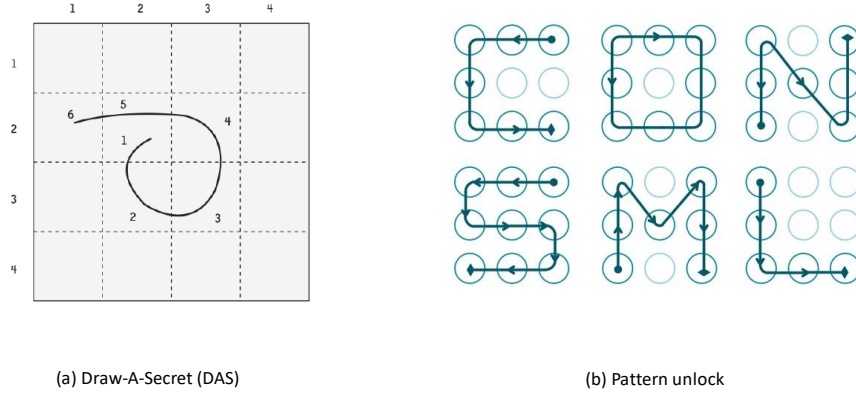


Figure 2.4: Purely recalled-base examples: (a) from [147] (b) from [148]

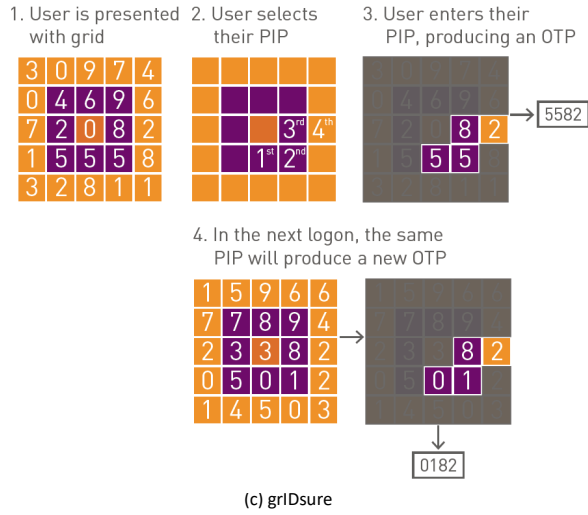


Figure 2.5: Purely recalled-base examples: (c) from [149]s

In the final instance, another crucial matter in purely recall-based graphical passwords which should not be underestimated is the ability of the user to draw sketches.

In order to limit their use due to the previous weaknesses, new better techniques have been studied where the user is guided by the image in remembering the password.

Cued recall-based

Cued recall-based schemes are based on the utilisation of graphical elements as hints to support the users' recall. This type of systems are frequently loci-metric, because the user is required to identifying specific locations within the image, but draw-metric exceptions exist, for example BDAS (Background DAS) [16], represented in Fig. 2.6 (a).

Click-points mechanisms (e.g. *Blonder* and *PassPoint*, respectively in Fig. 2.6 (b) and Fig. 2.7

(c)) employ images as a reminder for the secret, which can be assigned by the system from a library or, in some cases, provided by the user, with the only condition of being sufficiently complex. Obviously, click-points have to be inserted in the right order and have a tolerance margin, in view of the fact that users could make small imprecisions. For this reason, it becomes crucial the type of discretization used, i.e. the system acceptance of the entered click-points compared to the original points, for instance robust discretization, centred discretization, and optimal discretization are possible alternatives [13]. In addition, users tend to choose ordinary click-point patterns,

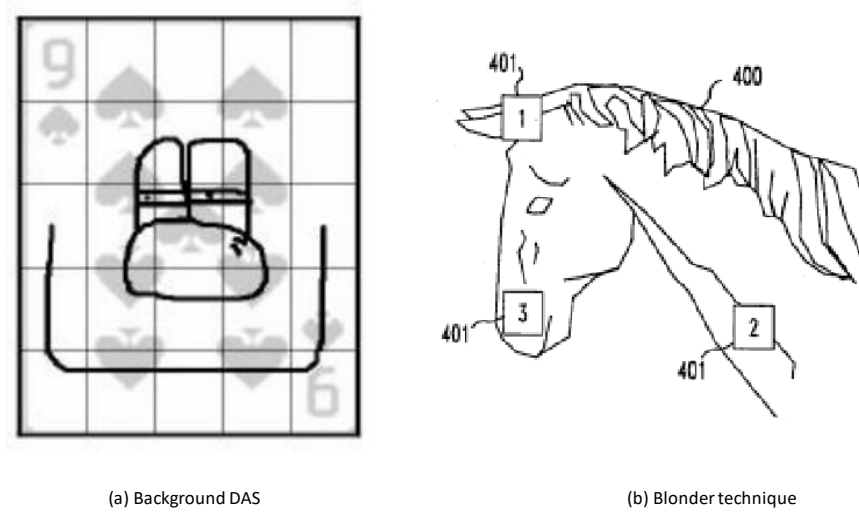


Figure 2.6: Cued recalled-base examples: (a) from [150] and (b) from [151]

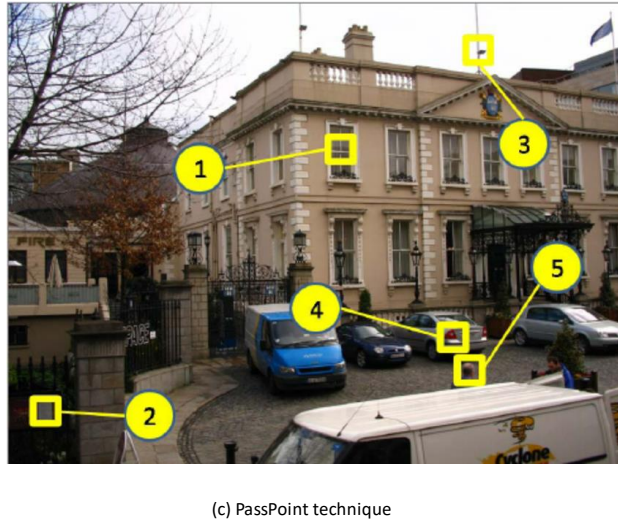


Figure 2.7: Cued recall-base examples: (c) from [152]

which have to be avoided in order to provide an adequate security level.

In this regard, Chiasson et al. proposed the so-called *Cued Click-Points (CCP)* system (Fig. 2.8 (a)), which relays on the utilisation of different images for each click-point and in case of error a user-unrecognizable image is represented, precluding access to any attacker who does not know the picture sequence. Although this mechanism eliminate standard patterns, it arises a hot-spots

problem. For this reason, Chiasson et al. presented a second solution, known as *Persuasive Cued Click-Points (PCCP)*, which represent the leading technique of this type of graphical passwords (Fig. 2.8 (b)). In the creation phase, the system reproduce a blurred image, except a minor random area in which the user is supposed to choose the click-point; while the image is completely clear in the login phase [13].

Despite the graded improvements, all the aforementioned schemes share vulnerabilities to

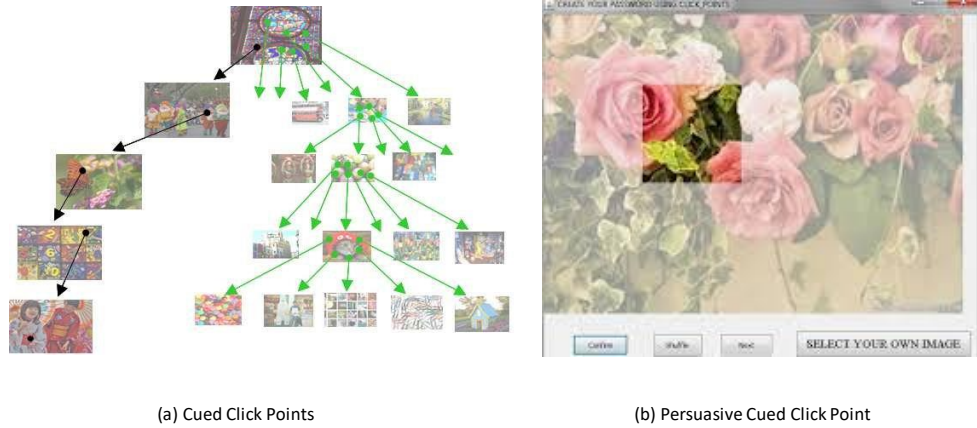


Figure 2.8: Cued recall-base examples: (a) from [153] and (b) from [154]

shoulder-surfing and malware, as well as MITM and phishing attacks. Furthermore, the number of available click regions is limited and as a consequence the keyspace result minimal, not providing an ideal level of security [17].

Recognition-based

Recognition-based schemes are the most suitable for image utilisation according to the several studies proving the undeniable human ability to effortlessly recognized pictures previously seen, even for an exiguous period of time. Defined as cogno-metric systems or search-metric systems, generally, these mechanisms require the users to identify a group of figures observed in the secret creation phase, within a larger set of distractor images [16].

Although they are characterized by a better memorability to the rest of the knowledge-based mechanisms, they have several weaknesses. First of all, most schemes offer a password space comparable to a 4-digit PIN (approximately recall methods are comparable to 8-character passwords), which is useful in particular environments, but it does not offer a valid substitute for common text passwords, with respect to security.

Moreover, it is important to notice that it would be best practice to assign random images to the users, due to their predictable behaviour. In fact allowing the users to choose their images reveal human tendency to be influenced by attraction, race and familiarity, causing severe security concerns.

Furthermore, in practice, image recognition schemes will not work well on small screens (e.g. palmtops) because of the requirement to simultaneously show multiple images. Indeed, the displayed grids can contain a minor number of pictures (e.g. 9), making it easy for an attacker to guess the secret in a few thousand random guesses.

The most popular recognition-based scheme is *Passfaces* (Fig. 2.9 (a)), in which the user has to select a limited number of face pictures presented by the system. During authentication, grids

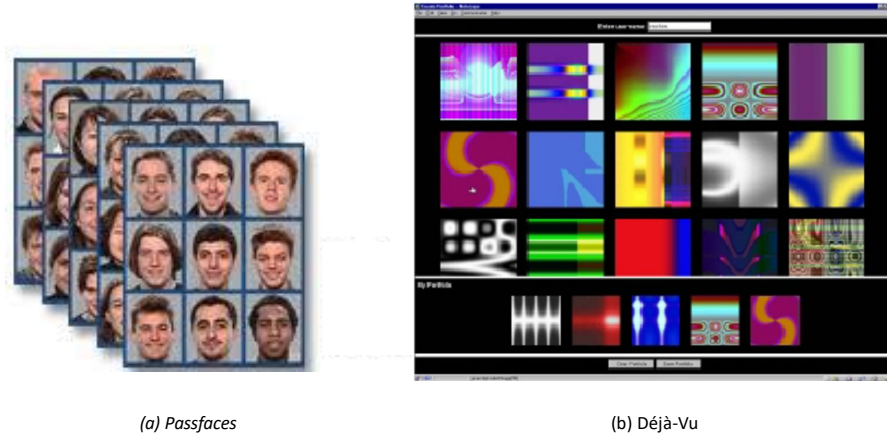


Figure 2.9: Recognition-base examples: (a) from [155] and (b) from [?]

are displayed for each of the previously indicated photos, filled with resembling images. Nevertheless, in order to achieve a level security comparable to 8-character-alphanumeric password, 15 or 16 rounds with 9 faces each are necessary, causing slow and tedious login [14].

Another example of recognition-based graphical password is *Déjà-Vu* (Fig. 2.9 (b)). It is based on abstract images and photographs rather than faces. Random art representation are used to make it more difficult for users to write down their password or share it with others by describing their images. Similarly, it would seem difficult to identify images belonging to a particular account based on knowing other information about the user. Problems resulting from predictable user choice remain possible, for example due to users favourite colour.

In the years, innumerable systems have been examined and proposed, always with minor improvements trying to eliminate recognition drawbacks. For instance, *Cognitive Authentication* scheme (Fig. 2.10 (c)) intended to be safe against spyware and shoulder-surfing [27]. The scheme is based on two simple rules, i.e. if the image on which the user stands on was in the set of pictures observed in the registration phase, then move down; otherwise move right. The user has to mentally trace a path, until reaching the right-most end or bottom end of the panel, with which a number is associated and it represent the secret. In order to authenticate, the user has to correctly answer with the number to a question. Another example is *Use Your Illusion* (Fig. 2.10 (d)), where the the distortion of the images is intended to protect against social engineering and shoulder-surfing attacks [28].

2.3 Ownership-based authentication

Ownership-based authentication is characterized by the physical possession of an hardware device, generally referred as *token*, whose principal purpose is to enhance the password system and establish a second line of authentication. Tokens can be a secure storage device containing passwords (e.g. bankcard or smart card) or an active device, which produces one-time passcode, either time-synchronous or challenge-response (i.e. on request). For this reason, strong authentication tokens are capable of performing cryptographic calculations on a dynamic variable, even based on symmetric-crypto-graphic algorithms parametrised with a secret value or key.

Ownership-based schemes have not been widely used, owing to usability issues, supplementary costs, support and replacement difficulties, in addition to the need for server changes and the

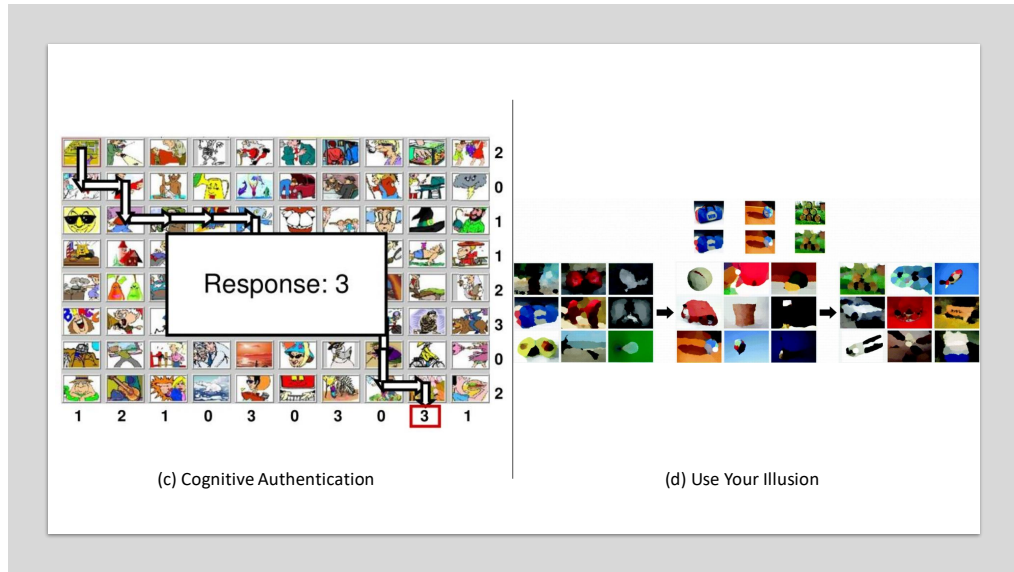


Figure 2.10: Recognition-base examples: (c) from [140] and (d) from [160]

necessity of diverse token for each account. Their utilisation is limited exclusively to extremely major-importance accounts, such as in banking, transport and eventually parking and hotels [6]. As a consequence, they are tamper-resistant in packaging and a specific hardware disables the token, in the event that it is tampered and if the maximum number of attempts is exceeded. Although tokens provide secure remote connections even in potentially non-secure environments, the major inconvenience for users is to remember to carry each token for the different applications [18].

Security tokens differ according to the type of password provided:

- *Static password*, the token contains an unvarying and unique password, which is directly transmitted whenever required, with any effort from the user, who cannot visualise it. It is obvious that it can be vulnerable to replay attacks.
- *Synchronous dynamic password*, the token creates new passwords, established by a temporal-key algorithm, at regular time intervals. The time key is imposed by the internal clocks of the control server and token, which must be synchronized.
- *Asynchronous password*, the token produces an One-Time Password password from cryptographic algorithm on user's request.
- *Challenge response*, the token respond to the authentication server public-key-encrypted challenge (e.g. random number or data), with the decrypted challenge, proving the possession of a copy of the matching private key.

The security tokens are distinguished not only by the methodology used to generate the password, but also by the methods of communication with the central control system. In the following sections, tokens are divided into four different categories.

2.3.1 Disconnected token

Hardware-based tokens are pocket-size battery-powered devices with their own display and occasionally a keypad, which, in some cases, is reduced to a single button. Generally, the presence of the keyboard derives from the fact that the token is protected by a PIN.

Most disconnected tokens rely on a one-time password technique, that cryptographically generate

a new one-time password (typically a PIN) valid only for the ongoing session. For example, they are massively utilised by the banks, in order to implement a second factor of authentication (e.g. UniCredit Pass³).

These hardware tokens have no physical or logical connection to the client computer and indeed the user need to manually enter the authentication information provided via keyboard or keypad (Fig. 2.9).



Figure 2.11: Disconnected tokens examples: (c) from [161] and (d) from [162]

The advantages of hardware-based strong authentication tokens include a very high level of security, independence of both application and delivery channel (i.e. any driver installation is required). On the other hand, disconnected tokens have disadvantages concerning the presence of the display, the battery and the keypad, which force the token to a minimum size and volume along with a certain cost. In addition, they present practical limitations on the nature and the length of the secret, from the moment it must be entered by hand by the user.

2.3.2 Connected tokens

This category represent tokens that must be physically connected to the computer with which the user is authenticating. The authentication information is automatically transmit to the client computer once a physical connection is made, eliminating the need for the user to manually enter the authentication information. Nevertheless, the appropriate input device must be installed. The most common types of physical tokens are smart cards and USB tokens, which require indeed a smart card reader and a USB port (Fig. 2.12). It is worth noting that new form factors⁴ have been explored to reduce this reliance, such as Universal Serial Bus (USB) tokens that can plug directly into a USB port on a computer.

³Details at <https://www.unicredit.it/it/privati/internet-e-mobile/tutti-i-servizi-internet-e-mobile/domande-utili-e-assistenza/strumenti-sicurezza.html> in the section “UniCredit Pass”.

⁴According to the *Oxford English Dictionary* a form factor is the physical size and shape of a piece of computer hardware.

Smart card

Smart cards are wearable identification and authentication cards on which a microprocessor is embedded, generally capable of performing sophisticated cryptographic algorithms. Constituting a means for two-factor authentication, they are generally associated with a PIN or in peculiar cases a biometric factor, which allows the decryption of data inside of the smart card by the dedicated reader. It needs to be mentioned that the limited processing capability of smart card chips allow the adoption of exclusively symmetric cryptographic functions (e.g. 3DES and AES). Nevertheless, although it is known that asymmetric cryptographic functions (e.g. RSA) are processor-intensive operations, smart card chips are currently available with cryptographic coprocessors that allow asymmetric cryptographic functions to become a practical option.

Therefore, their capability to process information permit encrypted communications, with no need to export either the public or the private key which reside in the smart card.

As a consequence of their security advantages, smart cards are generally used for Single Sign-On (SSO) authentication, which consists in authenticate once for access to multiple systems, for example logon to Windows and a Unix based system as well as enter a building. Moreover, because of their broad applicability and a extremely practical form factor, smart cards are employed in a wide range of different applications, such as payments security (e.g. EMV-compliant bank cards), e-mail protection and electronic documents signature. Finally, in addition to the fact that if stolen it would be immediately evident to the user (as opposed to passwords), their design is particularly tamper proof, providing security against the use of specialised hacking software or the removal of the chip, which would be undoubtedly damaged in the process. On the other hand, relatively high direct and indirect costs emerge from the complex technical interface, which impose specific command structures and drivers, and the dependence on specific reader infrastructure.



Figure 2.12: Connected tokens examples: (a) from [163] and (d) from [164]

USB

USB sticks are nowadays commonly used and offer several benefits such as low cost, convenience, expandability, auto-configuration and hot-plugging. The interaction with the host according to the USB specification allows to not require either a display or keypad, nor a battery. Hence, USB tokens can be large produced in a cost-effective manner and in smaller physical dimensions, enhancing the portability. Furthermore, USB smart tokens are very versatile and can have various memory capacities to meet the needs of end users. Their main purpose is to overcome some of

the major disadvantages of smart cards by combining into a single hardware device the functions of both a smart card reader and a smart card.

USB-based smart tokens are suitable for use in any scenario where important data and applications require a high security level. In particular, certain USB tokens store digital signatures, fingerprint details, or other biometric data, which could be used as cryptographic keys. Disadvantages of USB tokens include the need to install a driver prior to use, specific security issues (malicious software can impose the token to perform security sensitive operations without the user awareness) and for PKI-based USB tokens⁵ high cost and a need for large amounts of data to be exchanged [18].

The most widely used USB tokens are the Yubikey and Security Key, by Yubico, a privately held company founded in 2007 in Sweden which has become a worldwide pillar of authentication⁶.

2.3.3 Contactless tokens

Unlike connected tokens, contactless tokens form a logical connection to the client computer, but do not require a physical connection. The absence of the need for physical contact makes them more convenient in respect of both connected and disconnected tokens. As a result, contactless tokens are a popular choice for keyless entry systems and electronic payment solutions, such as Mobil Speedpass⁷, which utilise radio-frequency identification (RFID) to transmit authentication information from a key chain token.

However, there have been various security concerns raised about RFID tokens after researchers at Johns Hopkins University and RSA Laboratories discovered that RFID tags could be easily cracked and cloned [4].

Another downside is that contactless tokens have relatively short battery lives; usually only 5-6 years, which is low compared to USB tokens which may last more than 10 years. Some tokens however do allow the batteries to be changed, thus reducing costs.

Although the most common form of electronic data-carrying device in use in everyday life is the smart card, based upon a contact field (telephone smart card or bank cards), the mechanical contact used in the smart card is often impractical. A contactless transfer of data between the data-carrying device and its reader is significantly more flexible. In the following sections, the technologies utilised to implement contactless mechanisms are analysed.

RFID - Radio Frequency IDentification

Radio Frequency IDentification is a relatively old technology, which use instead of contacts, magnetic or electromagnetic fields. In recent years, it has become increasingly popular and practical for new applications and settings (e.g. tracking, identification, access control and payment systems), as a result of modern improvements in chip manufacturing.

RFID systems are normally composed by small transponders, generally known as *tags*, attached to physical objects and transceivers, or *readers*. Tags consist of a small microchip for storage and computation, which could support strong cryptographic functionality, attached to an antennae or other coupling element and communicates via radio frequencies with a transceiver (Fig. 2.13).

They can be classified according to the power source, which determines both the tag's range and cost, in:

⁵PKI-based USB token supports Public Key Infrastructure environments, i.e. supports qualified PKI certificate implementation.

⁶Specifications of the products can be found at <https://www.yubico.com/products/>

⁷Speedpass was introduced in 1997 by Mobil for electronic payment. In the 1999 the company merged with Exxon to become ExxonMobil.

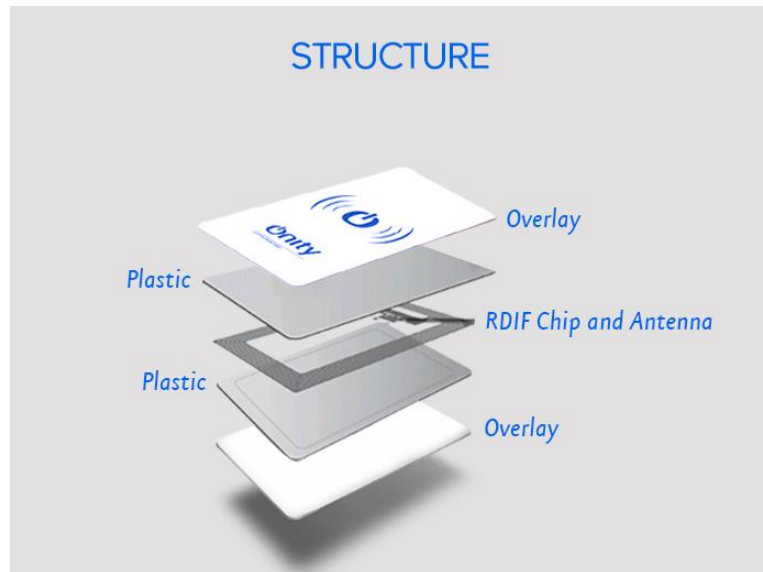


Figure 2.13: Example of a RFID card structure from [165]

- *passive tag*, in which the power is completely supplied by the reader and necessarily cannot initiate any communications. Hence they are the cheapest to manufacture and have the shortest read range.
- *semi-passive tag*, which have moderate range and cost, because of the embedded battery and the fact that they may only respond to incoming transmissions.
- *active tag*, which have the greatest range and cost as a consequence of an on-board power source and the ability to initiate their own communications.

Although the major efficiency gains offered by RFID systems, their wide deployment also incurs many security concerns and practical attacks at the cost of both privacy and security of individuals and organizations. Unprotected tags are vulnerable to physical attacks, counterfeiting, spoofing, eavesdropping, traffic analysis or denial of service. Moreover, as long as such RFID transponders are readable by an external reader, relay attacks can be performed.

Although their employment is mainly focused on inventory management, in the context of authentication this technology is increasingly exploited to replace magnetic or traditional identification badges. In fact, the short range of applicability does not represent a problem.

NFC

Near Field Communication is a consumer-oriented wireless proximity communication technology, which is based on and expands on existing RFID standards for contactless cards. Indeed, it employs magnetic fields along with induction to communicate data over a distance of centimetres (up to 10 cm) at low bandwidth. The automatic initialization, by simply touching a reader, another NFC device or an NFC compliant transponder, represents the major advantage of NFC, compared to other wireless communication technologies.

Consumers can have NFC functionality embedded in their regular phones, which consists of secure elements for performing secure transactions, using NFC devices as well as storing sensitive data in a secure environment.

Similarly to RFID, NFC system involves an active initiator device, which generate a magnetic field in close proximity to a passive target device, typically at about 4 centimetres or less.

According to the NFC Forum⁸, NFC technology is or may be used in the areas of access control, consumer electronics, healthcare, information collection and exchange, loyalty and coupons, payments and transport.

As a wireless technology, NFC may raise potential privacy issues and security risks, considering the possibility for attackers to attack an NFC device anywhere and without the consumer noticing. This type of devices are especially prone to eavesdropping and denial of service, prohibiting the use of the device or disturbing communication. Furthermore, as a result of its roots in RFID, it is vulnerable to relay attacks, adapted to NFC devices by just installing specific pieces of software. In addition, unencrypted data transfers, security holes in the software libraries or actual theft remain crucial concerns of this technology [19, 20].

Analogously to RFID, NFC is principally utilised as key or building entry device, but also to grant access to shared resources. For example, Lee et al. [171] proposed a NFC authentication mechanism to access printers, in order to allow the printing of documents according to the users' authority.

2.3.4 Mobile phone tokens

Two-factor authentication involving supplementary devices, such as tokens and cards, has been proposed to solve the password problem and have shown to be difficult to hack. On the other side, it arises secondary disadvantages, which include the cost of purchasing, issuing and managing the equipments; especially considering the fact that having to carry multiple devices increases the possibility of loss or theft [21].

In this day and age, mobile phone tokens are the most suitable solution to the problem of the excessive number of tokens a user might possess. In fact, the majority of the global population already have one and it can be considered both sufficiently secure and highly usable. Moreover, it is now habitual behaviour to constantly keep it in close proximity and always connected. Hence, it is possible to take advantage of its original features (e.g. SIM and SMS), or even install additional specialized software, i.e. vendor-specific and third party applications (e.g. Microsoft Authenticator app), in order to permit ownership-based authentication. In addition, the continuously improving capabilities of this type of devices allows to reduce the costs and to get closer to user needs [21].

The most popular implementation method provides the secret (typically a not excessively complicated One-Time Password) by sending SMS messages to a trusted number associated with the user, which has to manually copy the special authorization code from the mobile phone screen to the client terminal in order to authenticate (Fig. 2.14). The main advantage of SMS-based authentication is the exploitation of the cellular network, characterized by being separate and independent from the Internet network. Furthermore, it is possible to leverage the use of SMS messages in this manner, since the amount of crucial data is properly small to be communicated in a single SMS message.

The security of this scheme is based on the assumption that it is difficult for an attacker to steal the user's personal mobile phone and to attack the cellular network. Nevertheless, unfortunately, this method is characterized by a high susceptibility to MITM and Trojan attacks, along with phishing attacks, whose effectiveness depend on the content of the sent message. In addition, users could easily and accidentally reproduce a wrong sequence [22, 23].

In this regard Do van Thanh et. al [24] propose a solution to enhance the scheme usability, which correspond to automatize the process of copying the authorization code by securely connecting the mobile phone to the client terminal without compromising.

An alternative strong authentication technique which exploits basic function of mobile phones has been studied by B. Sodhi [25]. He introduces a cost effective and usable system, which instead

⁸According to the NFC Forum (nfc-forum.org) "The NFC Forum is a non-profit industry association whose membership draws from all parts of the NFC ecosystem."



Figure 2.14: Example of a SMS authentication from [166]

of SMS employs “dropped calls”, allowing to decrease the timing. The principal constraint is the fact that the phone has to be secure, i.e. no call should be made without the user’s knowledge. Therefore, this technique is vulnerable to an attacker capable to compromise the phone and initiate phone calls, besides DoS, which is not extremely relevant, since identifying attackers is considerably simplified compared to DoS attackers based on IP network [24].

The continuously increasing capabilities of smartphones allow researchers to examine an enormous variety of systems to be implemented on, which transform these mobile devices into actual authentication machines.

2.4 Inherent-based authentication

As previously mentioned, passwords, PIN and token based authentication systems have specific deficiencies that restrict their applicability in a widely-networked society. Throughout the years, researchers focused mainly on problems concerning memorability and usability, in order to provide an extremely ergonomic method, proposing biometrics as a third factor or an alternative to the two-factor authentication.

A biometric is a feature measured from the human body (e.g. fingerprint, audio or voice recognition, signature recognition, face recognition) which provide an unbreakable one-to-one correspondence between an individual and the data [4].

In order to acquire the characteristic and produce a digital representation, the system necessitate a specific biometric scanner, for example a fingerprint sensor or charge-coupled device (CCD) camera. In general, the sample acquisition, which includes a feature extraction stage discarding unnecessary and extraneous information, is completed with a quality analysis to ensure the reliability of the scan for successive stages [29]. The generic biometric phases are shown in Fig. 2.15. It is important to notice that the suitability of a specific biometric for a particular application is determined depending upon the requirements of the application and the properties of the biometric characteristic.

These type of systems are more reliable with respect of already addressed methods, as long as biometric traits cannot be lost or forgotten and require the user to be physically present at the time and point of authentication, making it difficult for an attacker to access without the user

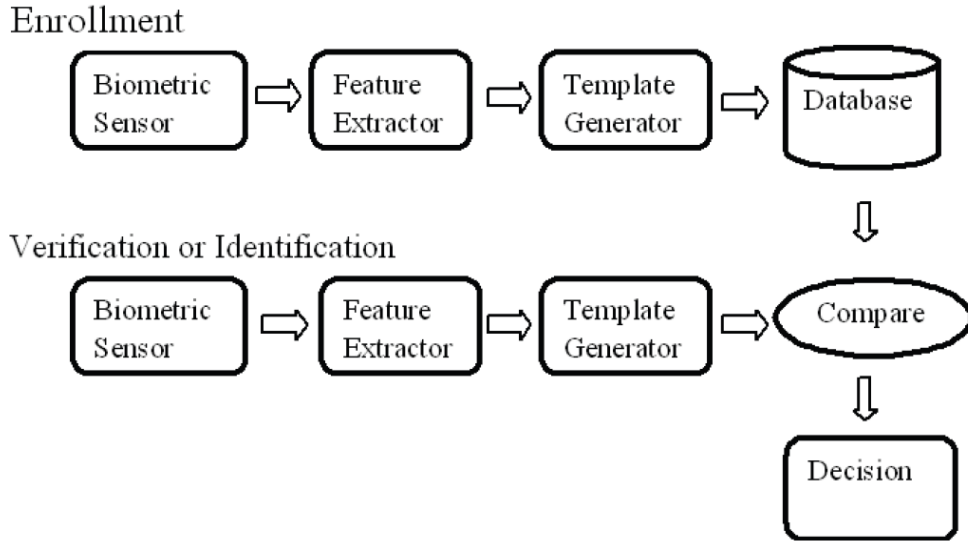


Figure 2.15: General biometric scheme [33]

noticing. Nevertheless, although a biometrics-based authentication scheme represents a powerful alternative to traditional authentication schemes, it has been proven not to be entirely secure, especially with regards to privacy. In fact, through varying levels of difficulty efforts, these unique characteristics can be copied or counterfeited to obtain unauthorized access to a security system, without any possibility of resetting, as long as they are distinctive traits of the user.

Moreover, in contrast to knowledge and ownership based authentication schemes, biometrics provide no perfect match and therefore it is necessary to adopt error rates to evaluate their performance, such as the False Rejection Rate (FRR) and False Acceptance Rate (FAR). The first is the percentage of authorized individuals rejected by the system and the second is the percentage that unauthorized people are accepted by the system [30]. The comparison metric for diverse biometric systems is generally the Equal Error Rate (EER), which represent the error rate at which FAR equals FRR, i.e. the false identification and false rejection rates are minimal and optimal.

In addition to the aforementioned issues, the biometric system is vulnerable to different types of attacks (Fig. 2.16), for example the underestimated zero-effort attack, i.e. the difficulty of a computer to distinguish particularly similar characteristics of two different individuals. In fact, depending on the acquisition method, environment and user's interaction with the device, biometric signals and their representations can vary dramatically, thus allowing the annulment of the uniqueness of the sample [31].

Furthermore, common attacks can compromise the security of this type of system, such as coercion, Denial of Service (DoS) or implementation of Trojan programs.

Researchers has identified two basic categories of biometrics:

- *physical*, which is based on personal physical characteristics, e.g. fingerprint, face, iris and hand;
- *behavioural*, which analyse user tendencies in movements and gestures, e.g. handwritten signature, keyboard dynamics (typing), voice and gait.

2.4.1 Physical biometric authentication

This type of authentication relies on peculiar physical traits, which are usually more accurate and reliable, because not affected by illness or stress. Nevertheless, various patho-physiological phenomena can cause variation in the traits, making the authentication impracticable.

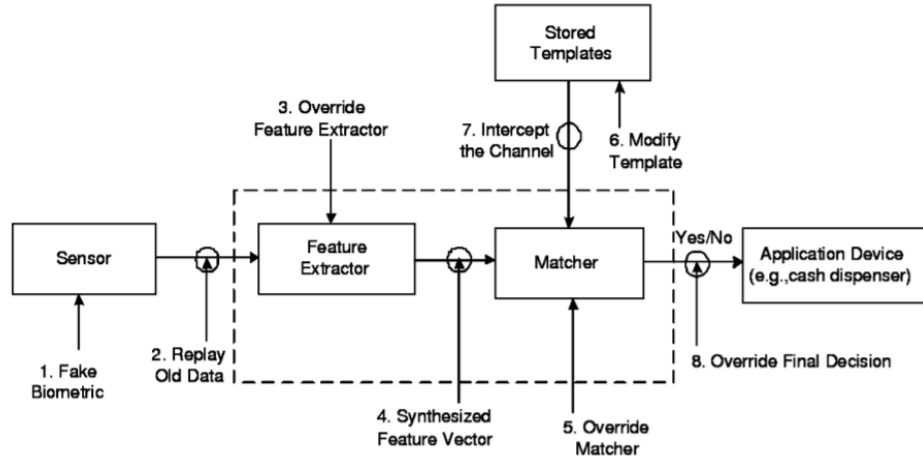


Figure 2.16: Vulnerabilities in a biometric system [29]

In the following sections the most popular physical biometric systems are described in more details.

Fingerprints

Fingerprint-based biometric authentication systems are the most popular and successful authentication techniques among other biometrics security methods, according to their ease of use, the reduced power requirement and the low cost of both implementation and optical sensor [33].

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, which is determined during the first seven months of fetal development and extremely unique of the individual, e.g. fingerprints of identical twins are different [29].

The main acquisition scheme relay on images of the fingerprint, from which the pattern of ridges and valleys are determined. Obviously, only distinctive sub-patterns and peculiarities are saved as an encrypted biometric key or a mathematical representation, in order neither to store the entire image nor to make it possible to be reconstructed (Fig. 2.17). This leads to a high level of security. Notwithstanding, obtaining high-quality images of finger patterns is a complex operation, because of the ridges and minutiae alterations caused by dirt, cuts, genetic factors, ageing, environmental or occupational reasons.

This mechanism is widely and globally utilised resulting from the implementation on mobile phones. In fact, for example, Apple introduced fingerprint unlocking as a feature for iPhone 5s in 2013, promoting the acceptance of this authentication technique worldwide.

Face Recognition

Facial recognition authentication systems are nowadays vastly implemented and globally accepted, since they represent the most spontaneous human identification method and because of the contactless and non-invasive process. Furthermore, the continuously increasing sophistication of core components and digital camera technologies, with competitive prices, constitute a crucial contributing factor to the strong emergence of face recognition systems [34].

Computer face recognition has the main purpose to detect individual features (e.g. eyes, nose, mouth and head outline) and define a face model based on the position, size and relationships

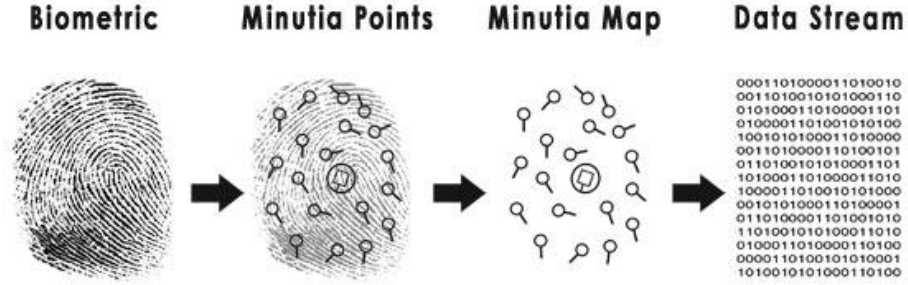


Figure 2.17: Fingerprint authentication method [167]

among these features (Fig. 2.18).

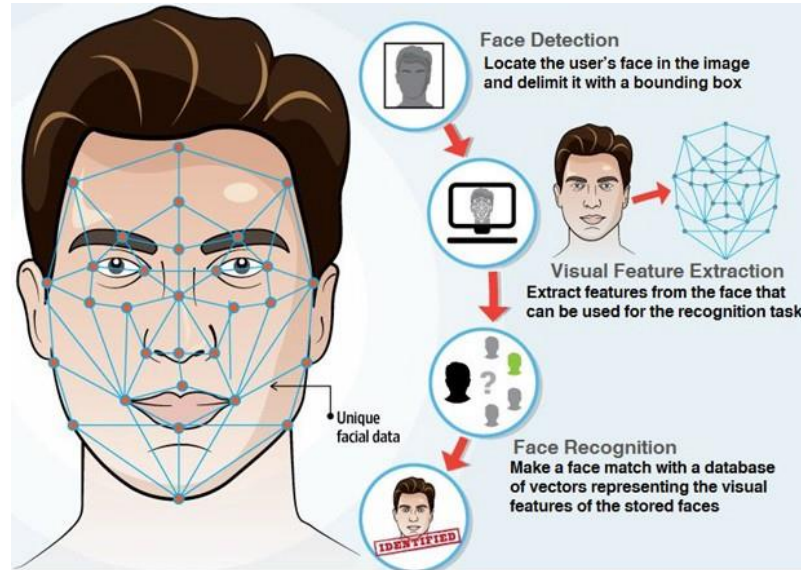


Figure 2.18: Face recognition authentication method [168]

Over the years, two main facial recognition techniques have emerged [35]:

1. *2D face recognition algorithms*

It is founded on Eigenfaces, which is a PCA (Principal Component Analysis) method, where face images are transformed into a minor set of characteristic feature images, called "eigen-faces", which are the principal components of the initial training set of face images. The recognition algorithm create an overall average image, based on the training set pictures and then compares to it the actual facial image, projected into the subspace spanned by the eigenfaces, calculating differences of the features. This mechanism has multiple advantages, including rapidity and reduced dimensions for both memory for identification and image

template. On the other hand, in addition to the limited information of 2D images, it has been found to be sensitive to lighting, head orientations, facial expressions and makeup.

2. 3D face recognition algorithms

The exploitation of three-dimensional geometry of the human face permits to overcome the aforementioned 2D difficulties. It is important to notice that most range scanners capture both a 3D mesh and the corresponding texture, in order to combine the 3D outputs with the traditional 2D algorithms and obtain better performances. Recently, as a result of excellent accuracy-with-low-cost recognition prefabricated components, it has become more popular to implement depth perception, projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. Although its disadvantages, regarding processing large crowds templates and computational costs, it successfully overcomes problems, such as isometric deformations and significant facial orientation changes.

Notwithstanding the rising prevalence of facial authentication systems, a great part of the population prefer to underline its probable privacy issues, in addition to bias and reliability problems.

In a similar manner as the fingerprint system, the dissemination and acceptance of this mechanism can be attributed to the implementation on smartphones. Indeed, the most famous companies, such as Apple, OnePlus or Huawei, provide 3D technologies to their clients.

Iris recognition

Iris recognition authentication systems are considered the most suitable biometric solution owing to their considerable reliability among other systems. In fact, iris patterns are peculiar features of any individual, which miniature radial traits remain stable and fixed from first years of age throughout life. Compared to fingerprint, it is furthermore an unique characteristic considering that, as internal organ of the eye, is protected from the external environment by the cornea and the eyelid [36]. The generic biometric phases are shown in Fig. 2.19.

In scientific terms, the iris is the annular region of the eye bounded by the pupil and the sclera

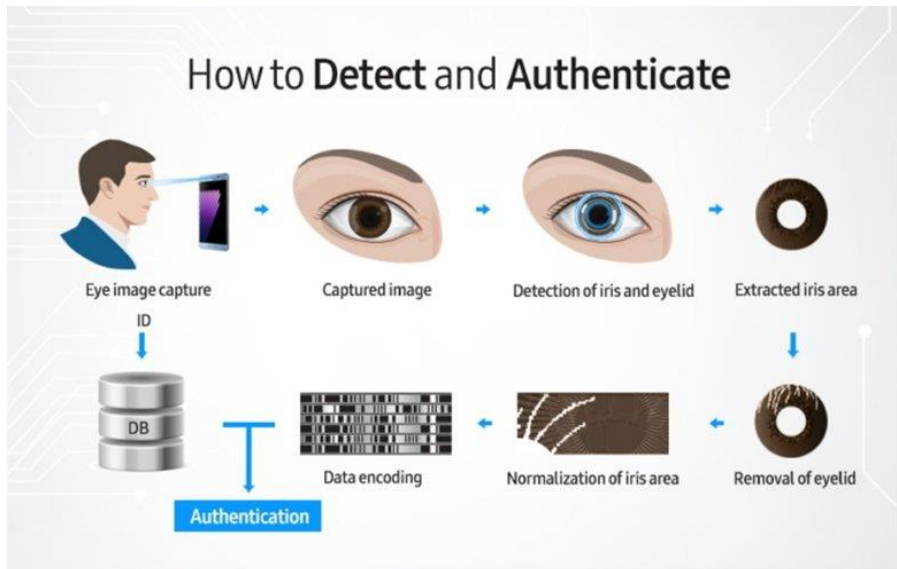


Figure 2.19: Iris authentication mechanism from [169]

on either side and its planar attribute provide relatively insensitivity to angle of illumination. Moreover intricate iris texture carries very distinctive information, such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette.

The main issue in automated iris recognition is to capture a high-quality image remaining non-invasive to the human operator. Although both the accuracy and the speed of currently deployed iris-based recognition systems are promising and increasingly user-friendly and cost-effective, they have manifested an extremely limited False Accept Rate (FAR) compared to other biometrics and possible elevated values of False Reject Rate (FRR).

Second important subjects of these type of authentication systems are the iris image acquisition and localization. It is nowadays impracticable to obtain a perfect iris image at first attempt avoiding acquiring the entire eye and the surrounding area, in addition to acquisition sensitive requirements concerning a wide range of edge contrasts, irregular borders and variable occlusion. In this context, particular importance is assumed by localization, which purpose is to extract the portion of the image derived from inside the *limbus*, i.e. the border between the sclera and the iris, and outside the pupil. Obviously a more-inclusive picture with expanded facial regions computationally burden the operation. Nevertheless, the ease of localizing eyes in faces and the distinctive annular shape of the iris facilitate reliable and precise isolation of this feature and the creation of a size-invariant representation [37].

Finally, even though it is extremely difficult to surgically tamper the texture of the iris, an ultimate problem arises from artificial irises (e.g., designer contact lenses), which have been demonstrated to represent a threat to iris-based authentication systems.

Although the iris recognition technology has been regularly employed by the military agencies, especially to buildings or facilities access, a new innovative utilization is being developed, which allows soldiers to securely communicate from the battlefield. A series of sophisticated technologies (i.e. R-100 camera and IrisAccelerator) from the Iris ID corporation⁹ have been included in the next generation of Combat Apps Tactical System (CATS) tablets, providing encrypted communication by capturing real-time biometric iris information [38].

Hand geometry

Hand geometry recognition systems have been employed in authentication for over 30 years, because of the uniqueness of the peculiarities of the human hand. Furthermore, although its mediocre security level, numerous advantages compared to other techniques can be identified, such as moderate costs, high speed performance, low computational complexity, ease of use and consequent massive acceptance.

Indeed, the human hand contains a wide variety of measurable characteristics (e.g. shape, size of palm, lengths and widths of fingers), which generally remain stable over time, albeit they do not vary significantly across the population [39]. Examples of features captured from the hand are showed in Fig. 2.20.

The mechanism requires a certain number of measurements of the human hand, with any particular obligation on the imaging optics, in opposition to systems based on fingerprint and iris, which respectively necessitate intact skin and specific illumination setup. Moreover, the acquisition is non-intrusive and do not demand a detailed extraction of the peculiarities, in addition to a very simple processing for the verification phase. It is important to notice that different factors, for example the surrounding environment or individual irregularities (i.e. dry skin), do not compromise this mechanisms as could be expected, while jewellery or limited capabilities (e.g. arthritis, swollen fingers or no fingers) can represent an obstacle to a correct information extraction [29].

A certain drawback of this systems is the massive physical size, which does not allow installation on certain devices, such as laptops. Although some devices have been modified to extract information from only a few fingers instead of the whole hand, they still remain significantly larger than other biometrics technologies, such as fingerprint, face and voice [30].

In this context a subsection of hand-geometry authentication systems has been studied, which include the extraction of only the palm information. Indeed, palm-prints possess a large number of

⁹<https://www.irisid.com/>

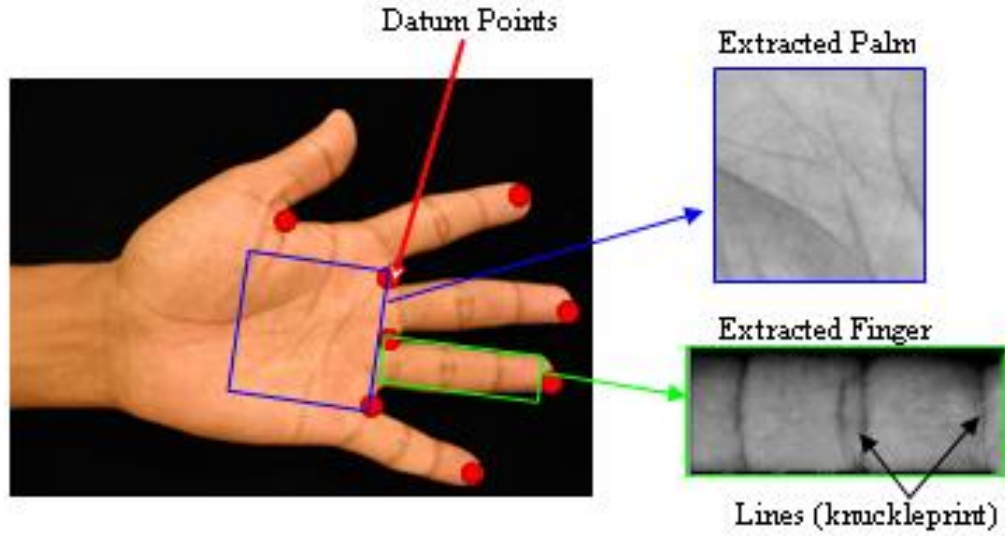


Figure 2.20: User extracted features for hand geometry authentication from [170]

creases, ridges and minutiae, similar to a fingerprint pattern, with the only flaw that can overlap [31]. In particular, the three lines known as the heart line, the head line and the life line are of greatest interest in palm-prints authentication (Fig. 2.21).

Since it is based on more peculiar characteristics of the human hand, this method requires higher quality images that make it possible to identify the features. Even in this circumstances, two different resolutions of palm images are available, which differ in the degree of specificity of recognition of the traits.

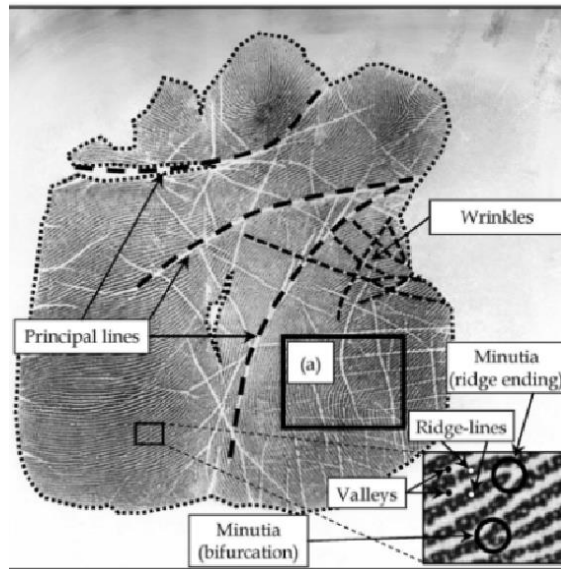


Figure 2.21: User extracted features for palm authentication from [32]

This technology was dominant on the market in the 90s, especially for employees attendance and access to doors. Although some companies still utilise this mechanism, nowadays iris recognition or fingerprints are preferred.

2.4.2 Behavioural biometric authentication

In order to meeting the needs of users to authenticate in a reliable, friendly and non-obtrusively manner, researchers have investigated methods that are based on people's behaviour. In fact, every human being in executing everyday actions develops his own personal way of operating, which can easily be employed in verifying the identity of a user. It is important to notice that this type of techniques are subject to the emotional state of the person, hence stress, fatigue, or illness can strongly affect their behaviour.

Notwithstanding the elevated variability of comportment over time and situations, which forces behavioural biometric systems to be more dynamic and with higher degrees of acceptance compared with other biometric mechanisms, they are extensively accepted because of their association with a non-intrusive and non-tedious mechanism [40].

Over the years, multitudinous behavioural biometric authentication techniques have been studied, especially based on individuals' motor actions.

In the following, the most commonly used systems are exposed in more detail.

Signature

Signature is globally considered the most effective method to identify an individual and indeed it is traditionally utilise in banking, financial transactions and document authentication. Moreover, as consequence of the extraordinary diffusion of PDAs and tablets, online signature has become a solid, convenient and accessible biometric option [40, 43].

Essentially two different typologies of signatures have been identified in the literature:

- *static or offline signature*, which can be used for basic authentication (e.g. documents) since it provides the shape of the signature;
- *dynamic or online signature*, which considers additional information about dynamics of the signature, including the horizontal and vertical pen movement trajectories.

In order to capture the dynamics of the signature, which provide a more reliable signature method with respect to the traditional one, special hardware is required such as pressure sensitive pens and digitising tablets (Fig. 2.23). Several signature-related features can be collected by these type of devices, for example the speed, the bounding box, the number of strokes, the signing flow (i.e. global features) and also distinct sample points in the signature and the relationship between them (i.e. local features) [40].

The process consists in an enrolment phase, where the user provide multiple signature samples, which are taken as reference signatures (Fig. 2.22). In case of dissimilarities above a certain threshold in the verification stage, rejection occurs. The main drawback of this mechanism, apart from professional forgers, is the dependence of the verification performance on the amount of signatures available for enrolment and the dependence of the optimal threshold on the user.

It is essential to consider the emotional and physical state of the user, which can affect the signature, such as health, posture or even sleep deprivation, alcohol and intoxication. Furthermore, it has been proven that elders tend to modify their natural signature movements on digital screens, increasing the pen pressure, the letter size and the writing speed. Finally, hardware problems may be encountered, concerning signature boxes, lines or display size, which force the user to adapt the signature [44].

Keystroke dynamics

Keystroke dynamics is based on the analysis of the user's way of typing, monitoring the keyboard inputs and delineating typical typing rhythm patterns. In particular, specific measures such as keystroke durations, finger placement and applied pressure on the keys are considered in order to extrapolate the typing characteristics of the user (Fig. 2.24).

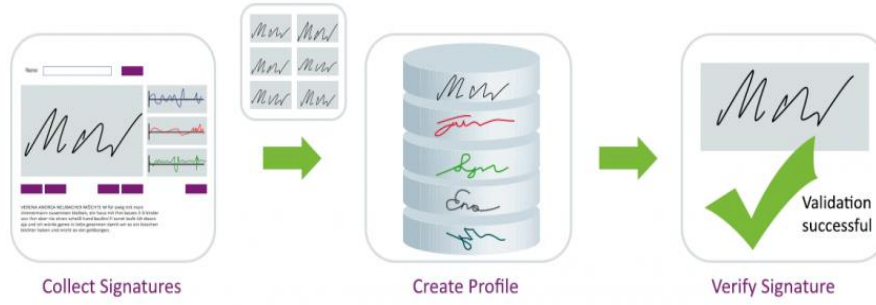


Figure 2.22: Signature mechanism from [41]



Figure 2.23: Dynamic signature PADs from [42]

The foundation of this technique is the opinion that writing fluency and flow vary from individual to individual, based on underlying cognitive processes. In the same manner as other behavioural biometrics methods, keystroke dynamic is affected by the physical and emotional status of the users. However, it is common that people typing-rhythm differs even between two immediately consecutive samples, despite they strive to maintain a regular way of typing.

The main advantages of this method is that it does not require neither any additional effort by the users, nor supplementary hardware, since the individual simply must type on the keyboard. Another interesting feature of keystroke is the possibility of continuous verification, obtained by monitoring over different periods of time the input rhythm of the user.

In recent years, research has focused in particular on the use of keystroke dynamics to avoid intrusion by impostors, who have become aware of a user's login credentials. In this context, typing rhythm detection systems have always been calibrated on short and fixed strings, i.e.



Figure 2.24: Keystroke dynamics example from [46]

username and password, which allows fixed-size feature vector and as a consequence a simpler implementation [45]. Nevertheless, on the other hand, fixed-size text systems raise significant problem concerning continuous verification, because, once logged in, it is not possible to monitor the user.

For this reason, latest keystroke dynamics methods have been developed to analyse long and freely typed text. Though, identify effective features for this type of text is arduous, because of the lack of prior information of the strings and the necessity to obtain sufficient amount of keystroke data.

Mouse dynamics

On the basis of keystroke dynamics, mouse dynamics has been studied in the latest years since mouse movement characteristics are considered to be as distinctive as typing (Fig. 2.25).

In particular, the user is requested to perform precise mouse operations on a specific graphical user interface in order to capture sufficient information to calculate mouse traits through statistical techniques [47].

The aforementioned action includes:

- general mouse movement;
- mouse movement followed by a click or a double click (Fig. 2.26);
- mouse movement for selection;
- no movement.

For each action it is possible to evaluate different factors, such as the average speed of distance travelled or directions, in order to construct the user profile. Several methods to acquire and extrapolate users characteristics has been studied, for example Gamboa et al. utilise username and a PIN number, both entered by means of an on-screen virtual keyboard, Bours and Fullupropose the acquisition through a maze, while Pusara and Bordleythrough navigating web pages [50].

Despite the different positive results comparable to face or voice recognition and the general optimism regarding this technique, the amount of data to be acquired remains almost unfeasible and the environmental conditions that can affect mouse mobility are underestimated. In fact, in the case of remote authentication users utilise different hosts from the one employed in enrolment and first verification, leading to rejections [50].

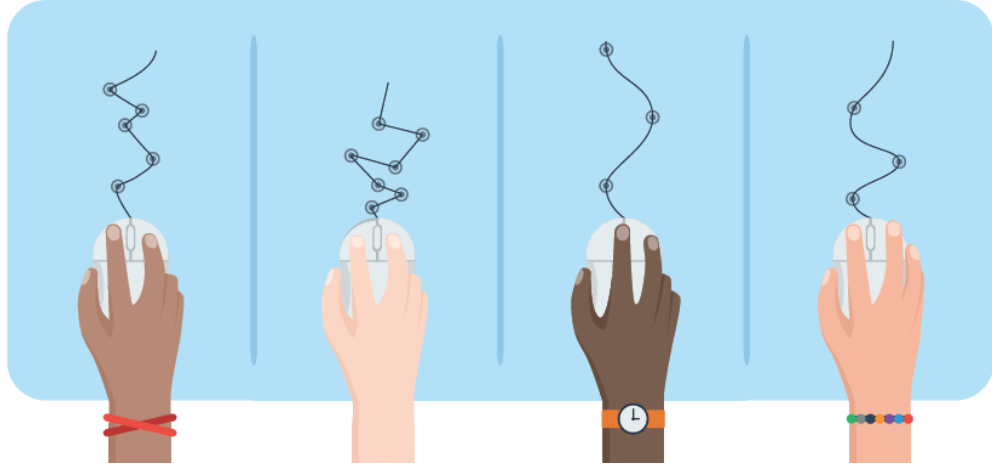


Figure 2.25: Mouse movements of different people from [48]

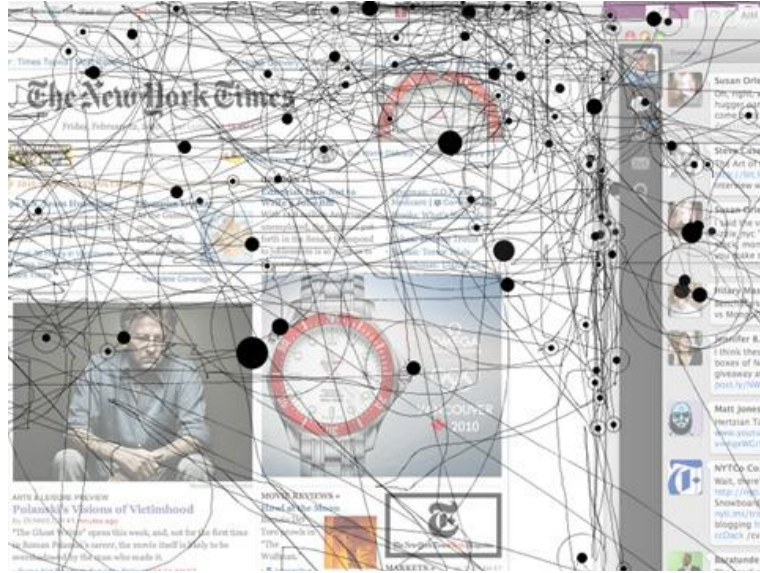


Figure 2.26: Mouse movements of different people from [49]

Voice recognition

Human voice is characterized by the shape and size of the person's vocal system (e.g. mouth, lips, vocal tracts and nasal cavities), which represent the invariant component of speech, and behavioural properties, which vary according to age, emotions or medical conditions (Fig. 2.27). Nevertheless, voice is not the most unique characteristic and it can be easily mistaken, hence it is considered not adequate for massive identification [40].

Three different verification text types can be identified:

- fixed text, i.e. predetermined word established in enrolment phase;
- text dependent, i.e. predetermined phrase;
- text independent, i.e. undetermined speech, which in general require larger spoken text, approximately of a duration of 30 seconds.

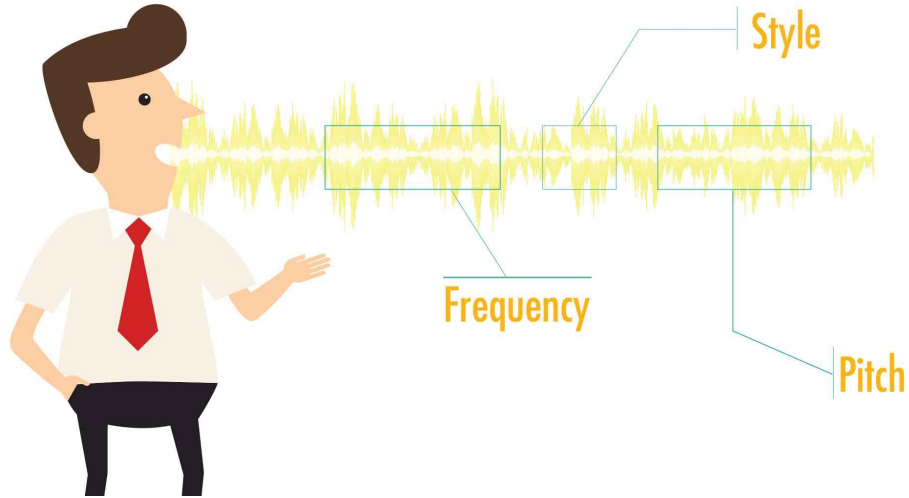


Figure 2.27: Voice recognition features from [51]

Voice authentication systems require basic cost-effective equipment, such as microphone or telephone to input speech, an analog-to-digital converter to digitize the spoken words, a high-powered computer and a database to store voice characteristics. An example of the voice recognition process is shown in Fig. 2.28. The main extrapolate feature in voice acquisition is the logarithm

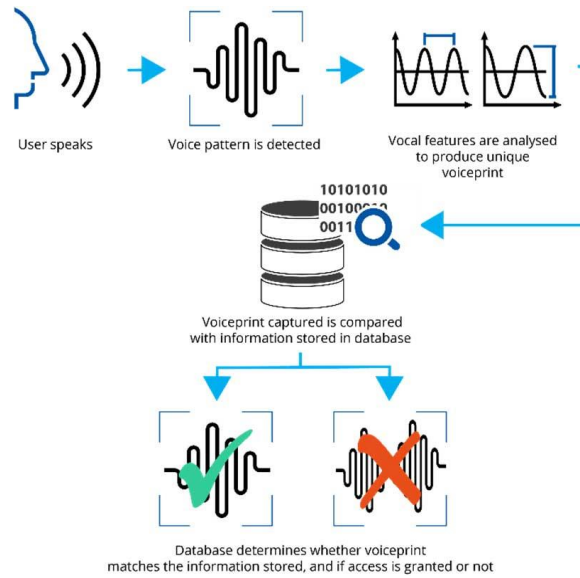


Figure 2.28: Voice recognition mechanism from [52]

Fourier transform of the voice signal in each band along with pitch, tone, cadence and shape of the larynx.

In some cases, in order to improve this mechanism, lips movement is integrated. The features captured include the mouth opening or closing, skin around the lips, mouth width, upper/lower lip width, lip opening height/width and distance between horizontal lip line and upper lip. This approach obviously necessitate to isolate the lip region from the video obtained from a camera, which increases hardware utilisation and therefore costs.

A disadvantage of voice-based recognition is that speech features are sensitive to a number

of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the communication channel.

An example of actual utilisation of this technology is the collaboration between IPI, the UK's leading Contact Centre Solutions and Aculab, a private UK company which provide media processing boards and software to the communication market, for the installation of the VoiSentry software¹⁰ to authenticate costumers by their voices, in order to reduce the annoyance of the identification and verification process [54].

Electrocardiography signals

Recent studies propose ECG waveforms as an alternative to other biometric authentication mechanisms, such as fingerprint, where the aliveness of the individual is not controlled and therefore the system can authenticate artificial copies of the biometric data. Furthermore, ECG can be collected from different parts of the body, such as finger, toe, chest or wrist, resolving the common problem of users with deformities or impairments [53]. An example of the ECG authentication mechanism is shown in Fig. 2.29.

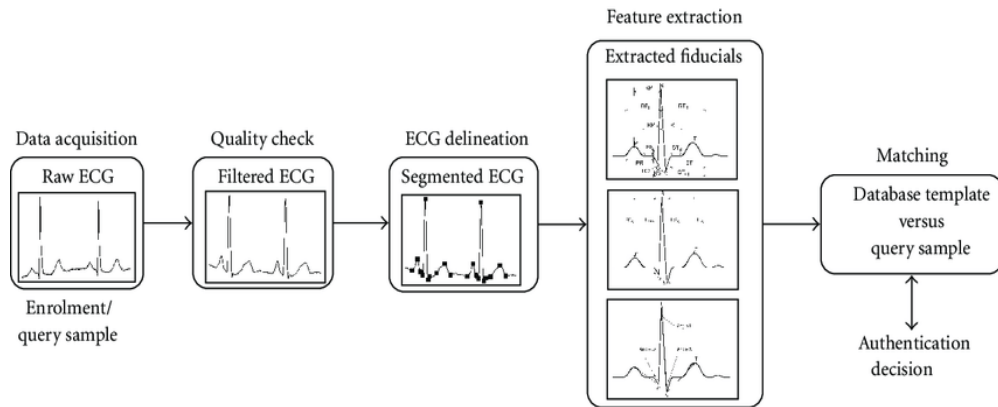


Figure 2.29: ECG authentication generic idea from [55]

According to [56], ECG has been classified in:

- *ECG biometric with Fiducial Point detection*, in which onset and offset points are detected in order to successively obtain wave characteristics, such as wave duration, amplitude, curvature, direction or slope. The authentication mechanism is based on the correspondence of real time extracted information with the enrolment data.
- *ECG biometric in the frequency domain*, in which various signal processing techniques (e.g. Fourier Transform, Wavelet Transform, Discrete Cosine Transform) are employed in order to produce the desired ECG features.

Keshishzadeh et al. [57] analysed ECG feasibility with outstanding outcomes, which resulted in high accuracy rate and low Equal Error Rate (EER). In their study, a combination of fiducial

¹⁰<https://www.voisentry.com/>

points dependent and independent methods for features extraction has been employed, providing, in this manner, a more accurate and robust ECG-based authentication system. Through the first method, which is based principally on the offset and onset points of the beats' waves, 55 features are obtained, including spatial, temporal and areal dependent features. The second method, which processes the ECG signal heuristically, produced for each beat sixty DCT coefficients exploited in the further classification. The total features are grouped into six set of features and the classification permits to verify or reject the claimed identity.

It is important to notice that only single-beat dependent features were extracted, in order to overcome the Heart Rate Variability (HRV) derived from stress or body movements.

A concrete issue of ECG biometrics is that no standardisation exists on the ECG feature wave boundaries, permitting to devices vendors to rely on proprietary definition of ECG wavelength boundaries. Therefore, it is a crucial problem considering that the points need to be exact since the slightest variation of fiducial point locations results in misclassification within the enormous domain of human population.

As previously mentioned, heart rate varies over time, depending on different physical or psychological condition and potentially it can cause the failure of authentication.

Furthermore, it is rare to find abnormalities which profoundly affect the ECG signal. For example, ectopic beat or premature beat are frequently unnoticed in a normal person.

In addition, ECG-base authentication is time-consuming, considering that to acquire a significant sample at least 20 seconds are needed (fingerprint acquisition requires less than a second).

Finally, the continuous technological advancement allows a contraction of the costs associated with the signal acquisition sensors. As a consequence, ECG-based systems can be embedded into portable devices, such as bracelets, as a module for multimode authentication or as a means of continuous authentication for the purpose of aliveness detection [56].

An interesting example of ECG-based authentication is given by the collaboration of Analog Devices, a world leader company in the field of integrated circuits, and B-Secur, a company specialised in ECG algorithm software implementation, for the introduction of an authentication mechanism in automotive vehicles. The technology is able to identify and authenticate the driver and his emotional state, controlling the readiness to drive [172].

2.5 Conclusion

In conclusion, user authentication remains a crucial problem which has no real solution. Users in general are not aware of the risks they may encounter and even in the case they have been informed, frequently voluntarily they tend to bypass security measures. On the other hand, developers continue to strengthen security constraints, consequently undermining the usability of systems.

In this context, the researchers has turned to the study and development of mechanisms which can partially exclude humans from the authentication process, eliminating the erroneous component derived from unsecure behaviours. The increase of IT systems in the everyday life of people, who authenticate multiple times per day, have imposed to move toward system-generated methods, which provide secure and univocal secrets, not subject to unconscious human models. These mechanisms are analysed in the following chapter.

Chapter 3

System-generated secrets

From the analysis concluded in the previous chapter, it can be deduced that the security of authentication systems does not depend uniquely on technical vulnerabilities, but it is clearly correlated with human behavior.

Although humans have proved to be unable to correctly manage credentials, both in terms of creation and maintenance of confidentiality, user-generated secrets (especially passwords) remain the most common method of user authentication, ignoring the main security drawbacks, which include predictability, reuse and memorability. Indeed, according to the Bank of North Dakota [58], “81% of hacking-related breaches leveraged either stolen and/or weak passwords.”. Moreover, the Australian Cyber Security Centre (ACSC) reported that five collections of stolen credentials (i.e. combinations of usernames, hashed and plaintext passwords), 1 terabyte in size each, have been distributed on hacking forum [59].

The inevitable predominance of passwords as a method of authentication and the evident incapability of users to generate invulnerable secrets, has made it essential to create new techniques that offer secure alternatives to user-generated passwords. As a matter of fact, considering the increasing complexity and diversification of the IT ecosystem, it is essential to implement new authentication mechanisms, which minimise the human erroneous factor and the resulting vulnerabilities.

In this chapter system-generated methods are described, with particular interest in different supportive memorability methods, which aim to overcome the principal memorability issue of these systems..

3.1 User-chosen and system-assigned secrets

Traditional authentication mechanisms require users to assume nearly complete responsibility for making their accounts secure, allowing them to create and manage their own secrets. As a consequence they result to be extremely predictable and rapidly crackable, due to the fact that humans are substantially incapable to randomly create anything without a realistic basis, and unconsciously tend to respect conventional patterns and impose some form of order to their creations.

For example, it is typical behaviour to choose ordinary dictionary words or inset numbers and special characters in predictable positions, during the generation of passwords.

To partially overcome this type of issue, more rigid constraints have been established in order to improve the security level of user-generated secrets. However, for example in the specific case of passwords, it is important to notice that strict policies, such as the inclusion of numerical digits and special characters or the prohibition of targeted words, might cause the user frustration. Moreover, it has been reported that excessively severe requirements do not increase the security

level, but rather affect the password memorability [60].

Furthermore, user-chosen secrets enable individuals to reuse them to a multitude of accounts, rather than inventing new ones, considerably facilitating the attackers

3.1.1 System-generated passwords

Over the years, in order to improve security and overcome the aforementioned weaknesses, a new method of automatically generating secrets has become popular.

For instance, the main target of this type of innovation are the alphanumeric passwords, since they still represent the principal authentication method exploited on a global scale. It consists in automatically providing users passwords, as a random combination of text and numbers, that meets the safety requirements.

As a result, however, serious problems of memorability arise because of the elevate complexity, which induce users to writing them down and leads to potential breaches in security.

An example is the *Persuasive Text Passwords* (PTP) system, which consists in a user-chosen password mechanism, which systematically enhances the generated string with random characters or word, and provides letter-recall schemes [61].

Another alternative in literature has been studied for decades, in order to increase password strength (i.e. its length, hence its entropy) and ease in memorization [62]. This concerns the so-called *passphrase* (Fig. 3.1), which consists in a provided sequence of words, in most cases extracted from specific dictionaries, separated by spaces.

Although the security and usability improvement expectations compared to passwords, it has been reported that passphrases are forgotten with same rates than passwords and written down with the same frequency. In addition, besides the multitude of options proposed, such as tolerance in typing, misspelling or words order, passphrases reported more input difficulties and errors. Furthermore, basic online password generators can be considered system-generated mechanisms, which are extremely disregarded because of memorisation problems. In fact, this type of generators is not developed to satisfy users' necessities, but only security requirements.

As previously mentioned remembrance of secrets, in particular of alphanumeric strings, represent

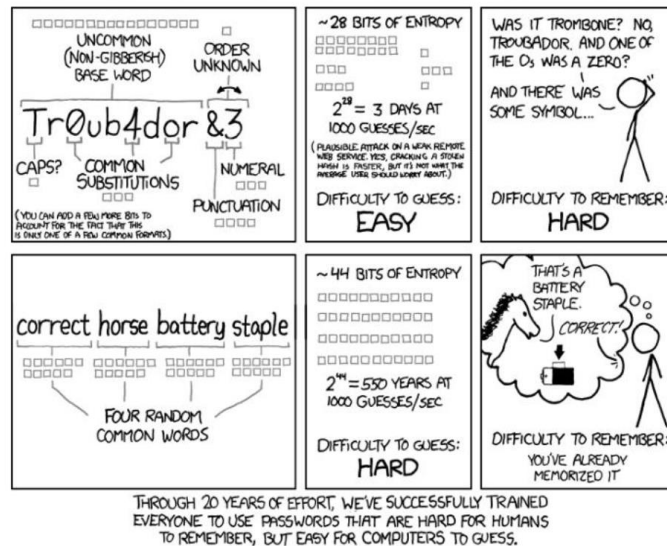


Figure 3.1: Passphrase example from <http://www.xkcd.com/936/>

one of the central challenges of user authentication systems. Indeed, complicated entry keys cause not only users' frustration (e.g. wasting time and attention in case of forgetfulness and possibility of being blocked) and difficulties in memorization, but also produce security breaches,

as a consequence of insecure behaviours, such as writing them down. In conclusion, although different schemes have been studied to meet customers' needs, any proposed solution was effective in facilitating users.

In order to improve the memorability of system-assigned secrets, different memorisation techniques can be utilised. In the following sections, they are analysed from the most common to the most innovative.

3.2 Enhancements to improve memorability of system-assigned secrets

Several studies has been conducted in order to overcome the limited storage capacities of human memory, which induce users to favour memorable, shorter and hence weaker passwords, composed by familiar words, names, dates and patterns [63]. Therefore, throughout the years, numerous researches have been concentrated on consistently facilitate long-term memorization in order to improve usability of authentication schemes. In fact, in the case of system-generated mechanisms, applying a memorisation method can solve the principal problem which affects these systems, which is remember the secret provided.

Considering that memory can be trained and strengthened, in the following sections the most prevalent enhancement memorisation techniques are discussed in more detail.

3.2.1 Pronounceable passwords

Among the earliest attempts to obtain more memorable passwords, it is remarkable the Gasser's proposal in 1975 in order to enhance the security of some Multics installations, such as the Air Force Data Services Center. He presented a random generator that assembled pronounceable syllables as a method of providing system-assigned passwords. The mechanism combines random phonemes which have to resemble English words, not considering context and grammatical rules. The majority of pronounceable password generators are based on Gasser's work, with different level of complexity of the pronunciation paradigms chosen. Indeed, the generator can base its password composition on basic restriction, such as not containing three consecutive consonants or vowels and no consecutive consonants can start or end the password.

As a consequence, although the generator is capable of creating passwords of any length, it is convenient to maintain a five to eight size, in order to facilitate memorization. Unfortunately, this practice increases the possibility of guessing attacks to succeed [62].

Some examples of this type of password¹ are:

- vonejotisixa
- f0z1c3g3sag0
- yuf3l1mu
- danafeki

3.2.2 Chunking

A different technique of memorization is partitioning the system-assigned password into small chunk. In fact, as the United States telephone number system demonstrates, it results simpler for humans to memorize more but shorter sequences of symbols.

The first chunking method to improve human information processing has been reported in Miller's

¹examples acquired with an online random generator at <http://randpass.floor500.net/>

work. After reviewing several memory experiments, he has established that humans tend to better remember $7 (\pm 2)$ elements and therefore the memory capacity could be directly increased by provide 7 chunks of a reduced number of characters, typically three (Fig. 3.2). It has been stated by further research that 9-character passwords, divided into three chunks, each of three characters, are the optimum solution to improve acquisition.

Nevertheless, generally, password generators are not implemented with partitioning features, which automatically divide the string in appropriate chunks with spaces or dashes. The separation become users' responsibility and hence it require additional cognitive effort, which can bother individuals [73, 74].

AJDui476LsiKm&Sp23

AJD|ui4|76L|siK|m&S|p23

AJD ui4 76L siK m&S p23

Figure 3.2: ALphanumeric string chunking example

3.2.3 Method of loci

The method of loci, also known as “*memory palace*”, is one of the ancient and most effective of the mnemonic strategies. The concept on which it is based can be found already in Roman literature, where Cicero suggests his lectors to insert elements to be recorder into places and remember the order of the locations.

Since that time, the method of loci has been adopted to memorize speeches and significant amount of information, especially when it is essential to respect a specific order. Therefore, the individual is supposed to retrace the path through the previously visualized loci in order to recall particular detail and hence utilise the journey as a cue [64].

This technique is particularly subjective since it is based on the users' imagination and consequently is founded on familiar settings, which permit a better etching in permanent memory. Furthermore, in order to produce a more memorable image, it is appropriate to train the individual to think to vivid and surreal scenes (Fig. 3.3). For example, it is simpler to humans to recall the shopping list if each item is associated with an unconventional scenery as for instance a fountain in the centre of the kitchen from which orange juice flows [65].

3.2.4 Link method

The link method requires to create a chain of things to remember, which are associated in pairs via completely abstract links. In a similar way as the method of loci, this technique is based on

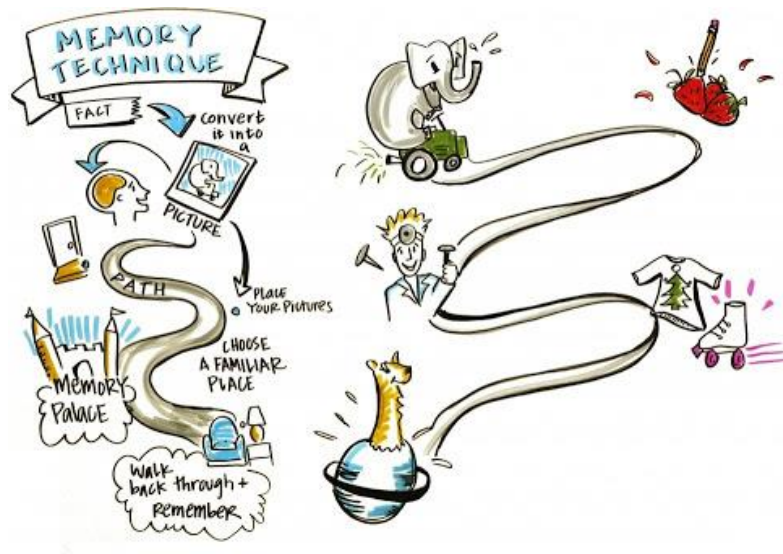


Figure 3.3: Method of loci mechanism from [66]

creating absurd stories that have two elements of the list of items to remember as protagonists, which therefore remain better fixed in mind (Fig. 3.4).

In order to create illogical stories, it is recommended to picture disproportionate objects (i.e. colossal or microscopic) doing something extreme, such as violent or shocking action.

The main limitation of this technique concerns the fact that if any element of the chain is forgotten, the entire list is compromised. Furthermore, it is user responsibility to remember the first item, even though it is sufficient to associate it with a specific place (e.g. the shopping list can be associated with the supermarket location) [67, 68].

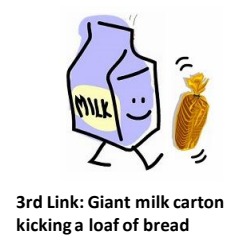
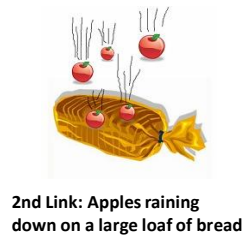


Figure 3.4: Example of the link method for a shopping list [69]

3.2.5 Exploitation of implicit memory

The previously examined techniques rely on the individual's capacity to consciously recall an information from the memory, which represent an extremely unreliable method. In fact, although it can be strengthened and preserved active, human memory is not infallible. Indeed, according to the article "Forgetfulness - 7 types of normal memory problems" published in Harvard Health Publishing [70], it is typical for the human brain to forget or alter memories at any age, even for healthy people.

During the last decades, human memory system has been studied with particular concern, principally focusing on the dissociation between two different kinds of memory systems. As a matter of fact, two distinctive learning methods have been identified, referred to by the terms [72]:

- *explicit or declarative memory*, which requires conscious recollection of previously experienced information, through recall and recognition;
- *implicit or non-declarative memory*, which allows the unconscious acquisition of information or abilities, as a result of previous experiences, in general through repetition or direct priming².

In the context of authentication, the evident difficulty of humans in remembering secrets by pure recall has increased researchers' interest in the implicit approach. In fact, implicit memory provides various advantages, such as complete dissociation with intelligence of the individual, a more lasting permanence, rapid response and resilience under pressure [71].

Therefore, it represents a valuable element to be considered and inserted in the development of alternative authentication systems, in order to address the inextricable problem of memorisation. As a consequence, numerous procedures has been experimentally investigated, including perceptual, motor and cognitive capabilities, with particular attention to repetition and direct priming (see 3.2.5 and 3.2.5).

As a matter of fact, the best practicable procedure to implement implicit memory effect in authentication mechanisms consists in an extended training phase in which users' perceptual system is stimulated in identifying or resolving ambiguous intuitive clues. The fundamental idea is that users' recognition performance increase when identical or similar objects are presented.

Although the most common perceptual implicit memory tasks are verbal (i.e. naming or completing fragmented strings), to grant secure authentication, the most interesting fields concern visual and motor stimuli, as a consequence of their peculiar characteristic of inability to verbally be exposed.

In the following sections, the aforementioned techniques are analysed in more detail.

Implicit visual memory

Several studies emphasise the major capabilities and accuracy of the visual memory system. Indeed, it has been observed through different experiments that participants are able to recognize a vast number of previously viewed photographs with high accuracy [75, 76].

Nevertheless, different studies on transsaccadic memory and change blindness have stated that a comprehensive and precise description of previously seen representations are impracticable for humans. In fact, it requires multiple eye fixations³ in order to define the global scene representation, with details and colour information.

²According to the American Psychological Association (APA) Dictionary of Psychology, the definition of direct priming is "cuing a response to a stimulus through prior exposure to the same or a related stimulus. The effects of repetition priming (e.g., changed speed of response, number of response errors) can occur without explicit memory of the first stimulus."

³According to Medical Dictionary (2009), eye fixations are defined as "Movement of the eyes so that the visual axes meet and the image of an object falls on corresponding points of each retina. This provides the most acute visualization of the object."

Furthermore, localist-minimalist theories consider visual perception limited in time and space to the object on which attention is paid, with a maximum of three or four additional items, which are captured and retained in the short-term visual memory. As a result, exclusively the information about targets are stored in long-term memory, in the form of an abstract, semantically-based, non-visual representation.

Moreover, although it is common belief that perceptual details decrease passing from short-term to long-term memory, latest researches stated that the context of the object of interest is unintentionally memorized in long-term memory and subsequently recalled to improve performance of successive visual searches [75, 76].

Therefore, it can be concluded that visual information acquired from attended objects during scene viewing is stored in memory whether or not the viewer intends to remember the information and consequently high expectations in the field of authentication concerns implicit visual memory, guaranteeing exploitation of this natural human mechanism to design new methods that do not require any cognitive effort by the user.

Contextual cueing Accordingly to the visual memory theory proposed by Hollingworth and Henderson, which argue that attention to an item is necessary to generate a visual short-term memory representation, researchers focused on visual context information, which facilitates localization and recognition of objects in complex displays [76].

Contextual cueing permits to rapidly identify a target in the midst of a series of distractors, progressively increasing users' performance over repeated displays of the image. In order to capture the focus of an object in an image, in addition to exclusive visual feature (e.g. colour, orientation or size) which may characterized it, context is fundamental to guide eye movements on the target. Indeed, it has been reported that attention and eye movements are directed to saliency areas of the representation, facilitating an observer's ability to acquire or react to objects or events within that area of a scene, with no explicit requirement to learn the displays [77].

With the increasing focus on large-scale implementation attempts of graphical authentication methods, studies on implicit acquisition of visual memory are becoming significant in the field of secure authentication, with the aim to design improved schemes in both usability and security.

In this regard, amongst the first authentication mechanism based on implicit visual memory is noteworthy *MooneyAuth* [78]. The authentication scheme is based on mooney images, i.e. ambiguous black and white images with limited properties, which represent a single object (Fig. 3.5).

The user is trained in the enrolment phase with a set of mooney pictures of which the solution is shown for a limited period of time (approximately 3 seconds), while in the authentication phase it is required to label both primed and non-primed pictures. The user is authenticated if the number of successful tags exceed the threshold of the score algorithm.

It has been demonstrated that, besides high memorability and complete absence of user bias (images are chosen exclusively by the server), this scheme is resilient to computer vision algorithms and guessing attacks. On the other hand, as most of the graphical methods, it is vulnerable to shoulder surfing and phishing attacks.

Another authentication method based on visual memory, in particular on the concept of contextual cueing, is the so-called *Tacit Secret* [80].

The system is based on the implicit memorization of a set of displays, which are repeated during the registration and hence compose the user's secret.

The task consists in identifying the letter "T" in the midst of letters "L" and press the arrow key corresponding to the orientation of the target letter (Fig. 3.6).

Since each display is shown for an extremely limited period of time, the success of authentica-

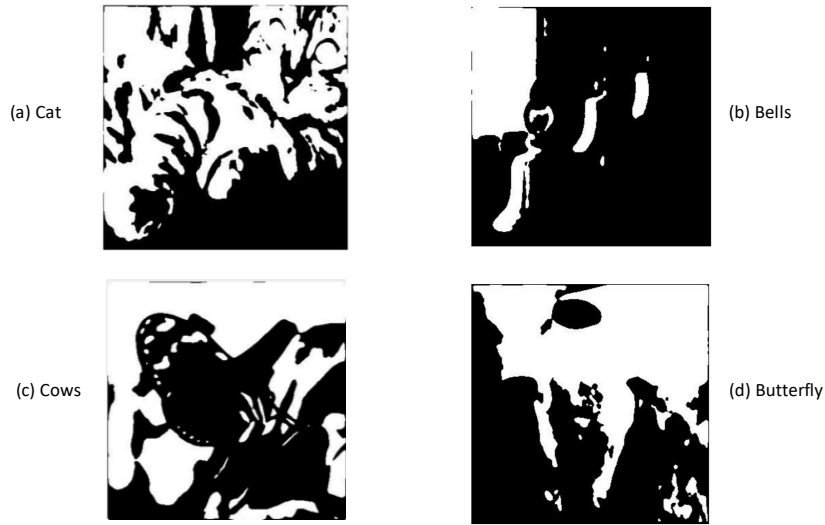


Figure 3.5: Examples of mooney image [79]



Figure 3.6: Tacit secret display example from [80]

tion relies in the user's ability to find the target promptly and proving in this manner to have performed the training phase. Furthermore, in order to restrict the possibility of attacks, the authentication sequence of displays is enriched with random novel screens and only one chance is given to the user to click the right button. For this reason, this mechanism is based on a score algorithm which authenticate users who demonstrate to know at least the enrolment sequence by performing high successful rates.

It has been demonstrated that this authentication system is sufficiently resistant to coercion attacks, guessing attacks and phishing attacks.

Implicit motor memory

This type of implicit memory, known as *procedural memory*, is responsible to encode, retain and afterwards recall actions that underlie motor, visuospatial or cognitive skills. Typical examples

of procedural memory are riding a bike, driving a car, walking or writing.

This technique has its foundations on the fact that humans tend to automatically perform an operation learnt through significant number of repetitions, enhancing performance by means of experience or practice. In scientific terms, this peculiarity is the result of the interaction of the synapses, which is strengthened with each replication, making the procedure automatic. Therefore, the principal characteristic is the complete absence of conscious thoughts, which determine the sequence of movements necessary to complete the operation.

The main advantages of this type of memory are endurance and arduous volatility, in addition to an extremely rapid re-learning rate, which ensure in this manner a remarkably reliable memory mechanism [81].

In authentication, this mechanism is exploited in order to create fast and secure authentication, without any effort on the part of the user who acts without thinking about it.

In particular, in recent years, a new technique referred to as “*gamification*” has been taken into consideration, which consists in introducing gaming as a learning method in non-gaming domains. The principal examples of success of this technique can be found in education, where it assumes different denominations such as “Serious Gaming”, “Edutainment” or “Learning Games”. Nevertheless, despite the excellent results found in this field and the very high expectations of improvement which it can bring in IT security, very few attempts have been made [82].

The mechanism has the purpose to present authentication in the form of a game, in order to allow users to not have the burden to recall any type of secret or action, but merely playing a game they were trained to.

The exemplary authentication system based on this factors has been proposed by Bojinov et al. [83], inspired by the famous game “Guitar Hero” (Fig. 3.7).

During registration, users are tested in maintaining an approximately 70% of correct typing,

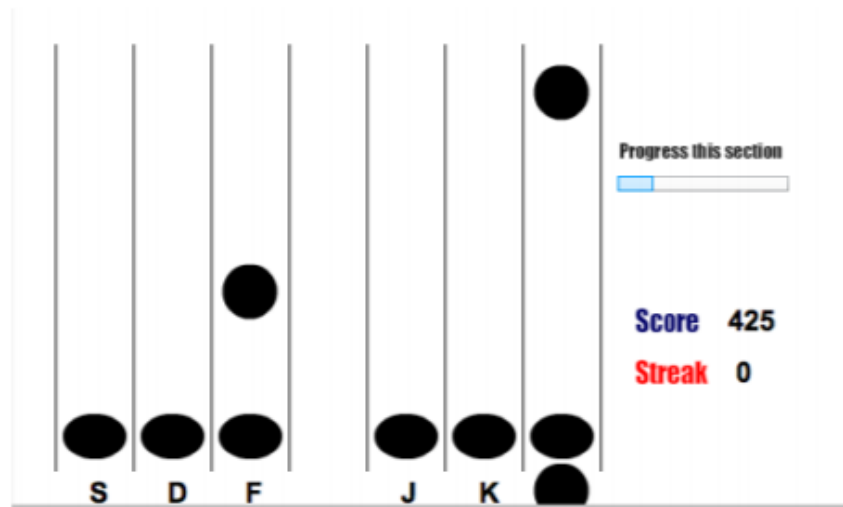


Figure 3.7: Bojinov et al. [83] authentication system

increasing the speed of the descent of the dots if the threshold is exceeded or reduce it in case of difficulty in being successful, in order to not frustrate users. The peculiar feature of this system, which relies on SILS (Serial Interception Sequence Learning) task, is the unconscious learning by the user of a predefined system-chosen sequence, which is repeated during the game and increases performance. In the verification phase, the game consists in a succession of portions of the sequence used in training combined with new parts, in which the user will obviously have worse results.

Although the elevated security level of this system, which is resistant to guessing and coercing attacks, the major disadvantage concern time, in fact in order to obtain satisfactory results

training requires 30-40 minutes and authentication 5-10 minutes.

3.3 Conclusion

In conclusion, due to the various vulnerabilities of user-chosen authentication mechanisms, system-assigned methods represent a necessity. Nevertheless, as a result of the detachment from the human instinct to be inspired by personal information for the creation of secrets, the critical problem of memorability has been emphasised. Consequently, although these systems allow to reach a high level of security, the scarce usability perceived causes user rejection.

For this reason, in this chapter, different memorisation techniques were examined, in order to provide a solution. Among those, the most interesting and promising one is the exploitation of implicit memory, which permits the user to make no cognitive effort neither during memorisation nor recall.

Chapter 4

Usability evaluation

In the previous chapters various authentication mechanisms were analysed, with their strengths and weaknesses. It emerged that the vulnerabilities do not depend uniquely on technical breaches, but similarly on the users attitude towards the systems. Indeed, the human component is a fundamental aspect to be considered in the development of a system, as determines its eventual success or failure. Therefore, it has become essential to evaluate not only the security of the mechanism, but also its usability, as the indication of the possible users perception of the system.

In this chapter, the various usability evaluation methodologies and metrics are analysed. In particular, it was considered relevant to present new objective metrics, which can provide truthful assessments, devoid of any unreliable human influence.

4.1 Usability definitions

Since 1975, thanks to the publication of J. H. Saltzer and M. Schroeder [85], usability has been recognized as an integral and fundamental component of security systems, as it has been argued that inadequate usability leads the systems to be insecure [86].

In the past decades, additional great recognition was given to usability for the success of the software products in the marketplace, even though cost and performance constraints remained the main concern for designers, developers and clients.

In this context, it has assumed the uttermost importance to find a compromise between the different elements which contribute to the success of a system, i.e. functionality, performance, cost, reliability, maintenance and usability.

Unfortunately, although usability has currently been recognized as an important software quality, one of the most significant problems is the lack of clarity of the concept. As a matter of fact, various definitions has been stated during the years and nevertheless no consistent standard is nowadays provided [87].

In first instance, the *IEEE Standard Glossary of Software Engineering Terminology* (IEEE Std.610.12-1990) in 1990 defined usability as:

“The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component.”

Concurrently, the *Directive 90/270/EEC of the Council of the European Union* stated the minimum safety and health regulations required for computer working [87].

Afterwards several ISO standard has been published [87]:

1. *ISO/IEC 9126* (1991), which delineate usability as:

“A set of attributes that bear on the effort needed for use and on the individual assessment of such use, by a stated or implied set of users.”

where “*attributes*” represents software product attributes and not user interaction attributes. Although the definition is the result of a system-centred usability concept, it is possible to notice the first influences of a more contextual perspective of usability supported by human factors experts. Further, in 2004, the standard was extended in order to meet the ergonomics needs dictated by the ISO 9241 standard, with a section on quality in use [?].

2. *ISO 9241-11* (1998), which provide a more specific definition:

“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.”

Written by human factor experts and not by software engineers, this definition represent usability as “a holistic assessment that combines multi-faceted qualities into a single judgement”. In fact, it is considered as the combination of three components, product of the interaction between users, goals, contexts and a software product [88].

Several further standards has been released in the following decades:

3. *ISO/IEC 9126-1* (2001), which in particular focuses on software applications, identifies usability as one of the six different software quality attributes¹:

“The capability of a software product to be understood, learned and liked by the user, when it is used under specified conditions.”

4. *ISO/IEC 25010* (2011), which reforms ISO/IEC 9126-1:2001 maintaining the software qualities with some arrangements, describes usability as:

“Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.”

In this case, usability is presented as both an intrinsic product quality characteristic and a subset of quality in use (comprising effectiveness, efficiency and satisfaction). Furthermore, different usability intrinsic sub-characteristics are defined, such as appropriateness, recognisability, learnability, operability², user error protection, user interface aesthetics and accessibility [88].

In addition to the aforementioned interpretation, a considerable number of diverse definitions related to more specific features have been issued [87]. As a consequence, although usability is one of the new major points of interest in software development, as it dictates the success of the product, no evaluation method has emerged among others due to its vague definition. Therefore, the choice of the usability evaluation technique became a difficult decision, considering the massive number of procedures provided by the literature.

Furthermore, in recent years, several studies have revealed a fundamental aspect of usability evaluation, which has been excessively undervalued, which is the context of use. In fact, usability can be considered a function of the context in which the product is used. Users, tasks and environment, which define the context, affect severely the evaluation of a system and an insignificant modification to one of these characteristics can completely reverse results. Therefore, it is fundamental in the evaluation of the usability of a system to consider every particular factor that defines the context of use, in particular during the selection of the metrics to employ [89].

In the following sections, employed usability assessment techniques and metrics are discussed.

¹Functionality, reliability, usability, efficiency, maintainability, portability.

²Degree to which a product or system has attributes that make it easy to operate and control - emphasis added

4.2 Background

In the modern scenario, where competition levels are incessantly increasing, the need to develop successful systems has made it essential to raise usability to one of the core components. In fact, usable systems improve user satisfaction, performance and productivity, as well as being a potential basis for managers to select between products.

Nevertheless, as a matter of fact, most importantly to succeed it is essential to implement a secure system, even if its complexity causes the user to perceive it as challenging. Therefore, it has become central, in addition to meet the users' requirements, to minimize the cognitive effort of users and the consequent frustration, which could lead to system failure.

For this reason, a trade off was forced between security and usability, which remain both indispensable for the success of a software product [90].

In this context, usability evaluation has become a consolidate procedure in the creation of modern systems, in order to provide an appealing product to the customers. The main purpose of this type of assessment is to detect possible usability problems in the various development phases of the system, employing different techniques in order to satisfy consumer's necessities and expectations. As an example, heuristic evaluation is optimal to be applied in the early stages of design, while user testing -which require the complete implementation of the prototype- can be applied in a successive phase.

In any case, according to usability experts, it is appropriate to adopt various and differing evaluation techniques, because in general usability assessment concerns a minor portion of the operations supplied [91].

In the following sections usability evaluation process is argued in more detail.

4.2.1 Usability evaluation

In early stages of introducing usability into computer science, usability was considered a mere technical factor (i.e. features and qualities of an interactive system), which could be achieved conforming to guidelines. The directives concerned for example naming, ordering and grouping of menu options, prompting for input types, input formats and value ranges for data entry fields, error message structure, response time and undoing capabilities.

In this initial phase, the fundamental idea was that human cognitive attributes were generically definite and therefore usability was an inherent binary property, derived from application of principles, formulated and validated by psychological experiments.

Nevertheless, in the early 90s, the opposite perception arose that cognitive attributes varied from individuals to individuals and consequently usability depended on users and on final objective.

As a matter of fact, usability became a central theme in the Human-Computer Interaction community and several evaluation methods were developed during those years, such as *user testing* and *heuristic evaluation* [88].

A usability evaluation is a process whose purpose is to measure the usability aspects of a system's user interface (UI) and identify specific problems. Although the procedure involves peculiar operation depending on the employed method, three typically common activities can be identified [91]:

1. *data acquisition*, which consists in collecting information concerning task completion time, errors, guideline violations and subjective ratings;
2. *data analysis*, which permits to detect usability problems;
3. *solutions or improvements proposal* to overcome the drawbacks.

It is necessary to specify that each method, which requires particular constraints, detects different usability problems even though is based on these cardinal points.

Although the guidelines published in the past decades are still maintained and followed, development of further methods was deemed necessary. Below some guidelines examples³ are presented [88]:

- Fast response, in order to not bother users, normal operations feedback should not exceed 0.2 seconds delay;
- Keeping data items short, in order to not require inappropriate effort from the user;
- Partitioning long data items, for instance telephone numbers partitioned into three chunks separated by a dash;
- Marking required and optional data fields.

Researches have developed different methodologies to test usability, which could be grouped in the following categories.

Automated evaluation

Automated evaluation is a technique which is preferred to perform in the early stages of system development, in order to promptly detect and correct trivial usability problems. Indeed, this type of assessment, as previously specified, must not be considered exhaustive or a suitable substitute for the most popular evaluation techniques; it is additional and complementary. Some of the advantages of exploiting automated evaluation include [91]:

- cost reduction, shortening the evaluation times through automatic tools inevitably reduces costs;
- extension of the functionalities evaluated, even though it remains unlikely to be able to evaluate every aspect of a system, automation certainly increases the coverage of tasks that can be assessed;
- reduction in the number of experts needed, in fact automating analysis or critique operations permits designers to perform an assessment;
- comparisons between alternative designs, through automated analysis approaches (e.g. analytical modeling and simulation) which enable designers to compare predicted performance for alternative designs.

Although it is extremely practical to document users' performance, it is complex to extrapolate from the results a level of satisfaction of the interaction. As a matter of fact, automated evaluation systems monitor users' input, focusing principally on objectives and intentions. Indeed, it is necessary to record users' interactions by means of video cameras, scan converters or screen capture programs, evolving automated evaluation into an intensive mechanism.

Promising developments in artificial intelligence favoured the idea of attempting to totally automate user testing by running surrogate users. Unfortunately, nowadays scarce experiments have been executed and proven overly simplistic, expensive and excessively specific to both the task tested and the application.

Notwithstanding the potential offered by this technique, it is scarcely investigated.

In the following some automated evaluation tools are briefly presented [87]:

- *DRUM - Diagnostic Recorder for Usability Measurement*
DRUM is a software tool created by K. Macleod and R. Rengger in 1993, for analysing user-based evaluations, which transmits results to an appropriate recipient, such as a usability engineer. It calculates diverse performance-based usability metrics, including:

³Examples taken from Smith and Mosier's 1986 collection commissioned by the US Air Force

- task time, which is total time required for each task under study;
- snag, help and search times, which concern the amount of time users spend dealing with problems, such as seeking help or unproductively hunting through a system;
- effectiveness, which is derived from measures of the quantity and quality of task output, and measures whether users succeed in achieving their goals when working with a system;
- efficiency, which relates effectiveness to the task time and thus measures the rate of task output;
- relative efficiency, which indicates how efficiently a general user performs a task compared with an expert user on the same system or with the same task on another system;
- productive period or the proportion of task time not spent in snag, help or search (i.e. the relative amount of productive work time).

- *SANe - Skill Acquisition Network*

The SANe measurement framework developed by N. Bevan and M. Macleod, in 1994, facilitate the evaluation of quality of use of interactive devices, proposing a user interaction model that describes tasks, dynamics of the device and procedures for the execution of tasks. The framework delineates a total of 60 different metrics, in particular 24 regarding quality measures. The results obtained from these 24 metrics are merged into five combined measures:

1. efficiency, which is determined by the estimated costs (e.g. total time) of executing user procedures;
2. learning, which reflects the number of states and state transitions necessary to carry out user tasks;
3. adaptiveness, which concerns the functionality of the device within a given application domain;
4. cognitive workload, which is influenced by controllability of the application, decision complexity (alternatives from which the user can choose) and memory load;
5. effort for error correction, which concerns the robustness of a device and the costs for error recovery.

- *AIDE - semi-Automated Interface Designer and Evaluator*

The semi-Automated Interface Designer and Evaluator tool, developed by A. Sears in 1995, permits to evaluate static HTML pages, in conformity with set of predetermined Web-page-design guidelines and even generate initial interface layouts. Moreover, it measures five different usability metrics, including efficiency, alignment, horizontal balance, vertical balance and designer-specified constraints (e.g. element positioning).

- *GOMS - Goals, Operators, Methods, and Selection rules*

The Goals, Operators, Methods, and Selection rules model created by B. E. John and D. E. Kieras, in 1996, describes the methods required to accomplish a defined purpose, which consist of the operation the user performs. Methods are organized in a hierarchical structure, where the final objective is constructed by the completion of sub-goals.

It is notable the selection procedure in case of multiple method choice to accomplish a purpose. In fact, GOMS has the peculiar characteristic of being able to select the appropriate method depending on the context.

Furthermore, another interesting feature concerns the introduction, as part of the description, of estimated time to accomplish a task. In this manner, it can predict aspects of the expert user performance, such as the total task time.

- *MUSiC framework - Metrics for Usability Standards in Computing*

The MUSiC project was created to describe software usability measures, integrated into the ISO 9241-11 (1998) standard. Although MUSIC framework include a considerable number of user performance measures, such as task effectiveness, temporal efficiency and length or proportion of productive period, it was necessary to introduce a more user-centred prospective, analysing additional aspects, such as user satisfaction or ease of use. For this reason,

the MUSiC project was extended to generate a questionnaire to assessing the usability of a software: SUMI (Software Usability Measurement Inventory). It consists of 50 questions, with three possible responses (i.e. I agree, Disagree, Don't know), centred on five dimensions of usability, i.e. helpfulness, control, learnability, efficiency and affect.

- *NIST Web Metrics*

The National Institute of Standards and Technology (NIST) Web Metrics, developed by J. C. Scholtz and S. J. Laskowski, in 1998, is a set of six computer tools and several metrics, which support a rapid, remote and automated testing and evaluation on websites.

- *EPIC - Executive-Process/Interactive Control*

The EPIC system simulates the human perceptual and motor performance system when interfaces with an interactive system. EPIC studies concern in particular users engaged in multiple tasks, such as using a car navigation system while driving. Using EPIC involves writing production rules for using the interface and writing a task environment to simulate the behaviour of the user interface.

Expert evaluation

Expert evaluation consists in an assessment of the product's usability by one or a group of usability specialists, who typically possess profound consciousness regarding general usability regulations and measurements. Indeed, this role is covered by people who have obtained a degree in the areas of human factors, cognitive psychology, experimental psychology or even industrial engineering [92].

Experts conduct an evaluation process, respecting specific customer audiences and tasks, in order to detect usability problems in a design at its initial stage.

The assessment can be performed employing the further methods [93]:

- *Heuristic evaluation*

Introduced in 1990 by J. Nielsen and R. Molich, it requires specialists to examine whether the heuristics are respected and with which grade. The heuristics are a set of established usability principles, which include according to Nielsen [94, 95]:

- “Visibility of system status: the system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
- “Match between system and the real world: the system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.”
- “User control and freedom: users often choose system functions by mistake and will need a clearly marked “emergency exit” to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.”
- “Consistency and standards: users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.”
- “Error prevention: even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.”
- “Recognition rather than recall: minimise the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.”
- “Flexibility and efficiency of use: accelerators- unseen by the novice user-may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.”

- “Aesthetic and minimalist design: dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.”
- “Help users recognize, diagnose, and recover from errors: error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.”
- “Help and documentation: even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user’s task, list concrete steps to be carried out, and not be too large.”

In addition, Nielsen specifies that the number of the specialists should be proportional to their level of competence; for example three to five regular usability experts are required in absence of more dexterous evaluators. Nevertheless it is complicated for developers to employ one specialist and particularly several times throughout the development cycles. Therefore, it represent one of the disadvantage of this method, in addition to the cost that this technique can achieve.

- *Cognitive walk-through*

In contrast with the holistic perspective of heuristics, cognitive walk-through is a task-specific simulation of the user’s problem solving process, whose aim is to discover usability problems, concerning mainly link labels, vocabulary and conventions on interface elements. It can be performed at any time during the development process and comprehends two different phases: the preparatory phase and the analysis phase. The first stage implicate the decision from experimenters of the interface, the expected audience and the tasks to be tested. In the second part, instead, evaluators walk through the Lewis and Polson’ steps⁴ to examine the procedure, questioning and gathering data at each step. Subsequently a final report of potential issues is compiled.

The technique has been used since the early 1990s, but it had two major limitations, i.e. the repetitiveness of filling out the forms and the limited range of problems the process found. Notwithstanding, as a result of further refinements and extensions, it has been proven to be an effective inspection method, which does not necessarily need cognitive scientists and usability specialists to be performed.

In any case, the cognitive walk-through remains a valid technique and it has been employed in different evaluation, such as the development of a multimodal tourist guide to Paris, an open source web-based digital library for the management and dissemination of social science research data, and a PDA-based game for teaching science [93].

- *Formal usability inspections*

It use a six-step procedure with strictly defined roles to combine heuristic evaluation and a simplified form of cognitive walk-through.

The inspection is performed by a heterogeneous group of specialists, including design engineers, usability engineers, customer support engineers and occasionally customers, who has different responsibilities according to the role assigned. At the final stage of the evaluation, an explicit rework meeting or document that commits to particular changes and solutions is composed. Therefore, it result more formal, technical and time-effective compared with the aforementioned methods.

The main disadvantage of this method concern recruiting a number of specialist from 4 to

⁴Lewis and Polson’s steps include:

1. The user sets a goal to be completed within the system;
2. The user determines the currently available actions;
3. The user selects the action that they think will take them closer to their goal;
4. The user performs the action and evaluates the feedback given by the system.

10, with different preparation, which determinate the successful completion of the evaluation [93].

- *Pluralistic walk-through*

Analogously to formal usability inspection method, the evaluation team consists of experts of various areas, such as developers, members of the product team and usability experts and additionally involve representative users. As a consequence, the not-completely-developed system can be instantly redesign.

In particular, the evaluation rely on 5 specific rules [93]:

1. inclusion of representative users, product developers, and human factors professionals;
2. the application's screens are presented in the same order as they would appear to the user;
3. all participants are asked to assume the role of the user;
4. participants write down what actions they, as users, would take for each screen before the group discusses the screens;
5. when discussing each screen, the representative users speak first.

The inclusion of users, in addition to bringing diversity in the evaluation, facilitated the experts in discovering usability errors.

Inserted in the Usability Professionals Association Body of Knowledge⁵, along with the first two previous approaches described, the pluralistic walk-through is employed in industry, as the upgrade of a graphics program to Windows NT demonstrate.

Expert evaluation is particularly crucial in the development of an interactive system, because it represents the last stage before the introduction to end users and therefore the last chance to correct errors before development is complete.

Involving users

A comprehensive assessment of the usability of a system is possible exclusively through the execution of different evaluation approaches. Several studies state that in order to detect the greatest number of usability errors is preferable to perform all the three types of evaluation (i.e. automated, expert and user testing).

Usability testing refers to the evaluation of a product or a service by a group of representative users. The evaluation in general requires users to complete selected tasks, in order to collect qualitative and quantitative data, which are further analysed for the assessment.

To run an effective usability test, it is proper to follow three fundamental steps [96]:

- development of a solid test plan;
- recruitment of participants;
- analysis and report of the results.

Considering the amount of resources involved, costs represent an important aspect of concern. In particular, the costs of the testing depend on the type of testing performed, number of the team assembled and of participants, in addition to the duration of the test (e.g. days).

Therefore, it is crucial to select the most suitable moderating technique based on the session objectives. In specific, the most common are:

⁵“The Usability Body of Knowledge is dedicated to creating a living reference that represents the collective knowledge of the usability profession. [...] The Usability BoK is derived from published literature, conference proceedings, and the experiences of practitioners accumulated over many years. It is a guide to existing resources, and will evolve as the practice of usability evolves.” from <https://www.usabilitybok.org/>

- *CTA - Concurrent Think Aloud*

Concurrent Think Aloud impose users to express their streams of consciousness (e.g. thoughts, expectations, decisions) aloud during the interaction with the system.

The real advantages of this approach are the elicit instantaneous feedback and the emotional response of the users, who reveal their thoughts while occurring [96]. On the other hand, it can affect usability metrics, such as accuracy and time on task. Furthermore, verbalizing during the attempt to complete a task could result challenging and influence user's behaviour [97].

- *RTA - Retrospective Think Aloud*

In order to overcome the problem of accomplish two actions simultaneously, the method of retrospective report has been considered.

In this case, after the session completion, participants retrace their actions and comment the procedure. In general, a video facilitate the users in recalling their behaviour, occasionally also registering eye-gaze patterns. Although this technique does not interfere with usability metrics, the entire duration of the session increase and particularly relevant can result in paucity of data, considering the critical issues of recalling past thoughts [96]. In fact, it is possible that imperfect memory can distort remembering and deform rationalizations and constructed explanations [97].

- *CP - Concurrent Probing*

Concurrent Probing allow the observer to demand follow-up questions when the participant attracts his attention during the think aloud. As a result, the understanding of participants' thoughts is immediate. Nevertheless, this attitude leads to the interruption of the natural thought flow of the user, affecting behaviour and time.

- *RP - Retrospective Probing*

In Retrospective Probing, the researcher takes notes of the stimulating observations and actions of the participants and at the end of the session demand follow-up questions. Although it does not interfere with usability metrics and the stream of thoughts of the user, the difficulty in remembering remains a serious problem that leads to unreliable data.

Moreover, typically at the end of the test, it is usual to subject the participants to a further questionnaires and rating scales, aimed at assessing user satisfaction (including confusion, frustration, and particular interface attributes, such as system responsiveness and meaningfulness of messages) [97].

Usability testing has the main purpose of revealing the level at which the system is able to meet the needs of the expected users. Unfortunately, in general the focus is on representative or selected aspects of the product, rather than on its entirety. Furthermore, in general participants are influenced by the environment, feeling compelled to impress or to neglect certain errors. It has indeed been found not unusual behaviour to not report difficulties at the final step of the test. Finally, additional flaws, caused by the limitations of time and resources, concern participants sample dimensions, which typically are inferior of a statistically significant number, and the selected number of tasks [92].

4.3 Evaluation location

An experiment can be set in the field or in a controlled laboratory. In both cases, the purpose is to collect information with the least contamination of results possible.

The environment selection is crucial and usually the laboratory is the most popular choice, due to participants' informed consent and privacy problems. In any case, insofar as possible and resources permitting, the most valuable approach remains the combination of both laboratory and field test. In fact, controlled experiments produce new approaches or hypotheses to be investigated in the field, and reversal [98].

In the laboratory

A controlled environment has consistently been the preferred choice. The main strength of this solution is the reduction of variability, which can cause unreliable results.

Laboratory usability testing emulates the expected real-world context of use in a controlled environment, employing equal equipment for every participant, who performs tasks with the same set of data. Nevertheless, it is important to notice that “*controlled*” implies users being isolated from contextual factors, i.e. distractions, such as interactions with other users and products which redirect their attention.

Therefore, the focal points to set up an adequate laboratory test are represented by the determination of the scenario, which has to be realistic, considering both the situation of use and the task to present, and the recruitment of representative users, who has to correspond to certain characteristics of the target audience [99].

Depending on the stage in the product development process, laboratory usability testing can assume two different connotations:

1. *exploratory testing*, which aims to detect problems in order to inform product designer and stimulate redesign;
2. *performance testing*, which aims to collect quantitative data (e.g. number, type and severity of users’ errors) in order to permit benchmarking.

Laboratory testing presents some limitations, in addition to the lack of context and users cooperation. For example, in general the user has to go to the designated location, increasing costs for the client. Furthermore, laboratory can be set up with video cameras, recording devices or other control equipment, which can influence user behaviour.

For these reasons, it is appropriate to adopt laboratory solutions in the case of dangerous or impractical location of the system, or for constrained single user systems which require controlled manipulation.

In the field

Field research has the main objective to extensively comprehend actions, objectives and needs of users in response to both documentation and the tested product. In fact, it consists in observing participants in their typical workplaces, such as home or school. In certain instances, it is possible that participants remain unaware of the test [98].

Although currently this solution is not widely employed, contextual inquiry and contextual design, along with ethnographic interviewing, have been typically exploited as qualitative methods by large organizations, which could invest significant resources in research for extensive projects design improvements. In fact, considerable issues concern field researching, such as budget, schedule and logistics, which represent the main obstacles to management acceptance.

Furthermore, remote product testing oblige the evaluators to travel to the field and organize the portable usability laboratories or in alternative obtain permissions to operate in local usability laboratories.

In order to address the aforementioned issues, remote software testing has been developed, which include several typologies of tools, such as Internet questionnaires, surveys, automated usage tracking, sharing software, desktop or video conferencing and live or collaborative remote evaluation. Moreover, it permits data gathering of a vast number of users, considering that allows to extend the target audience to who would be unable to come to the laboratory (e.g. people with disabilities).

Field testing is therefore recommended in longitudinal studies or in situations where context is essential, allowing to identify specific problems users encounter in ordinary activities. In fact, testing a system at home or in small business settings, can be revealing, since the computer, software or Internet service provider employed can affect the experience and hence the behaviour

of users, in addition to different distraction factors, such as work-space size, lighting quality, background noise or interruptions from family members and pets may also be factors [101].

4.3.1 Conclusion

Laboratory and field evaluation are complementary valuable methods, which represent basic element of the design process.

Intensely controlled environment of laboratory is preferred for summative evaluation, in order to control the certain defined usability criteria; while field observations are addressed to a more specific monitoring “associated with the integration of the product into the actual working environment” [102].

The growing interest in contextual research of IT systems has emphasized the relevance of environment on the usability of a product. In practical terms, notwithstanding an adequate representative user recruitment and meticulous selection of realistic tasks, conflicting results can be obtain in the laboratory rather than in the field, due to the impressive effects of physical, social and technical environments on usability.

4.4 Usability measurement

As previously mentioned, usability is a peculiar characteristic, which defines the interaction of users with systems, such as websites, software, devices and applications. As a matter of fact, it is a combination of different factors, including ease of learning, efficiency in use, memorability, subjective satisfaction, in addition to an intuitive design.

Therefore, it is impossible to declare a single measure to determine usability [103].

Furthermore, usability is particularly affected by contextual factors, such as intended users, design, technologies employed and the surrounding environment [2]. In fact, it is onerous to explicitly specify features and attributes required to the system to be usable, such as other system characteristics as functionality or portability.

The limitation concerning difficult in defining appropriate characteristics derives from a singular dependence of usability on the context of use. The interaction between the system and users is indeed significantly influenced by physical and organisational environments⁶, equipment (including hardware, software and additional materials) and tasks selection.

Therefore, it is fundamental for designers to consider in first instance the possible use cases in which the system can be exploited and attempt to identify and specify the components of the entire system which could affect usability.

Considering the critical importance of context of use in the decision of usability metrics, in the following section it is examined in more detail.

4.4.1 Context analysis

As already stated, usability evaluation is a crucial issue in the development of a product, considering that meaningful results can be obtained exclusively if the system is tested in representative conditions.

The contextual issue was addressed in the first instance in the late 80s by Whiteside et al., who experienced discrepancies between the results obtained in the laboratory experiments and the

⁶The physical environment Bad lighting or loud noise even the location of the product
the organisational environment the structure of the organisation, the way people work (individually and in groups),
the availability of assistance and the frequency of interruptions [102]

actual outcomes of the product when inserted in a real-world situation. As a consequence, they encouraged work in cooperation with the users in order to produce a result that is appropriate to the actual conditions of use in real world.

This new type of approach stimulated context configurations discussions, starting from strengths and weaknesses of laboratory and field studies and producing a serious determination to address context issues [102].

During the years Usability Context Analysis (UCA⁷) has become a fundamental operation of systems' development process. It has the main purpose to assist the systematic description of the specific context factors, such as users, tasks and use cases and the modus to be represented in the successive evaluation.

Analysis of the context is currently an essential prerequisite for usability research and involve the entire life cycle of the system. Typically, an initial early "context meeting" is arranged by an usability-backgrounded experienced facilitator, in order to discuss in generic terms the usability objectives and the intended utilisation of the product. A subsequent meeting is disposed to define user types and tasks for an informal evaluation, which purpose is to refine the requirements. Finally, an ulterior meeting establishes users and tasks for a further formal evaluation of usability goals achieved.

UCA involves a remarkably heterogeneous group of individuals, which should cover a relevant role in the system development process, with sufficient seniority influence on decisions. Nevertheless, the team must include a reasonable number of individuals typically from 3 to 8. Therefore, in addition to the facilitator, project managers, designers and user representatives must be present. Furthermore, potentially appropriate members can be introduced, such as quality managers, documentation managers and technical writers, training and user support managers, Human Factors professionals or certification and auditing responsible.

Recognizing that *context dictates usability* and systems can be considered usable only in a peculiar context, in order to ensure an appropriate investigation of context issues during the development, the MUSiC project has advocated 4 concrete principles [102]:

1. "*The usability of a product depends on its Context of Use*";
2. "*Products should be designed for specific contexts*";
3. "*Measurement of usability must always be carried out in an appropriate context*";
4. "*Usability measurements should always be accompanied by a detailed description of the Context of Evaluation*";

Notwithstanding the enormous influence of the context on usability hitherto stated, frequently evaluations are performed in inappropriate environments. The main reasons are the costs in terms of time and money to obtain the necessary resources (e.g. users and specialists), identify the real employment scenarios, the underestimation of the effects on evaluation results and the absence of a systematic method.

Furthermore, it has been challenging identifying a comprehensive list of context factors that impact on context of use.

According to the aforementioned composition of the context, based on three dominant factors, such as users, tasks and environment, Thomas et al. [102] in their guidance presented a hierarchical list of the most common affecting elements of usability of IT systems, divided in 5 major sections. All the proposed factors affect in particular two of the main usability components, efficiency and satisfaction.

⁷The original Usability Context Analysis Guide was a product of MUSiC (ESPRIT II project 5429 - Measuring Usability of Systems in Context), which developed a number of methods and tools to measure the usability of interactive systems.

The first section concern user's characteristics and it is further partitioned into different sub-sections, concerning different aspects of a target user. For example, in the *skills and knowledge* sub-section are involved:

- *Product Experience*, which consider the practical experience with the product or similar interfaces;
- *Input Skills*, which concern user's ability and familiarity entering data using various input devices (e.g. keyboard or mouse);
- *Linguistic Ability*, which is fundamental in the usage of the product and its documentation;
- *Training*, referred to the general IT or system-specific training received and the means by which the training has been received (e.g. formal training, video instruction or training manuals);

Furthermore, physical and mental attributes must be considered, in addition to the job characteristics of the user, in particular the job history.

The second section concerns tasks to be performed, in order to evaluate usability. It has been previously argued the difficulty to select tasks, which has to be representative for the entire system. The following characteristics should be considered in order to facilitate usability:

- *Task duration*, referred to the time required for the user and product to carry out a task;
- *Choice*, which concern user's decisional ability to select a specific product to conclude their tasks;
- *Physical and mental demands*;
- *Criticality of the task output*.

The last three sections concern environment, in its three facets, i.e. organisational, technical and physical.

In the organisational environment is important to consider elements regarding the structure (i.e. how job is managed), the attitude and culture of the workplace and finally the worker control (i.e. "The methods which are used to ensure that desired levels of productivity and quality are maintained"). More specifically:

- Structure includes:
 - *Group Working*;
 - *Interruptions*;
 - *Management Structure*;
 - *Communications Structure*, which refers to the main means of communication between colleagues and/or customers, and the relationships between these individuals.
- Attitudes and culture of the environment includes for example the IT Policies or the organisational aims .
- Worker control includes:
 - *Performance Monitoring*;
 - *Performance Feedback*, how do users receive feedback about the quality and speed of their work (e.g. weekly, monthly);
 - *Communications Structure*, which represents the process by which the rate at which workers perform their tasks is controlled.

The fourth section regards the resource utilization, such as hardware (i.d. user's equipment processor, storage devices, input and output devices), software (e.g. operating system and applications) and reference materials, in order to assist users in understanding the technical and system environment.

Finally, the last section concerns physical environment. It include:

- Environmental conditions:
 - *Atmospheric Conditions*, which could affect both users' and the technical system, in particular it refers to outdoor weather conditions, but also include the building;
 - *Thermal Environment*, which refers to thermal conditions of the workplace which affect performance of user and product;
 - *Auditory Environment*, which concerns distractions for the users or limitation in interpersonal communication, generating stress or annoyance, in addition to deformation of product's sounds;
 - *Visual Environment*, which represent the visual conditions of the workplace, affecting both user and product performance.
- Workplace design:
 - *Space and Furniture*, which include size, layout and furnishings and other items in the workplace, such as desks, screens, cabling, printers, etc;
 - *User Posture*, which refers to physical position adopted and the freedom of movement of the users;
 - *Location*, which concerns location of the workplace in relation to fellow work colleagues, customers, resources, target area of influence and even the user's home;
 - *Visual Environment*, which represent the visual conditions of the workplace, affecting both user and product performance.
- Health and safety:
 - *Health Hazards*;
 - *Protective Clothing and Equipment* .

4.4.2 Usability metrics

Although usability has been recognized as substantial software quality, standards failed in providing a unambiguous definition, resulting in a practically inability to establish accurate measures of evaluation. Furthermore, the importance of context of use affects the relevance of the metrics to evaluate. Indeed, the selection of appropriate measures and the level of detail depends on the objectives of the evaluation and the characteristics of the context of use. Therefore, it is in general necessary to include at least one measure of each usability component, in order to provide a reliable evaluation [87, 89].

Referring to ISO standards for usability definition, *effectiveness*, *efficiency* and *satisfaction* represent the three main components of usability [104]. In particular, they can be described as:

- *Effectiveness* as the “accuracy and completeness with which users achieve specified goals” [ISO 9241-11]. It can be estimated, for example, by values of quality of solution and error rates.
- *Efficiency* as the “resources expended in relation to the accuracy and completeness with which users achieve goals. Relevant resources can include time to complete the task (human resources), materials, or the financial cost of usage.” Moreover, learning time can be utilized as indicator of efficiency.
- *Satisfaction* as the “degree to which user needs are satisfied when a product or system is used in a specified context of use. For a user who does not directly interact with the product or system, only purpose accomplishment and trust are relevant. Satisfaction is the user's response to interaction with the product or system, and includes attitudes towards use of the product” [ISO 9241-11].
Typical indicators of satisfaction are attitude rating scales, such as SUMI (used in the MUSiC project).

Several researchers proposed additional characteristics to expand and refine the concept of usability, including qualities such as *learnability* (e.g. Nielsen (1993), Gilb (1996), Jones (1997),

Schneiderman (1998) and the MUSiC project in Bevan et al. (1991)) or *security* (e.g. ITSEC-Information Technology Security Evaluation Criteria and ISO/IEC 9126) [104]. As a result, a comprehensive usability model can be generated, organized in three different levels, i.e. characteristic, sub-characteristics and measures, represented in Fig. 4.1.

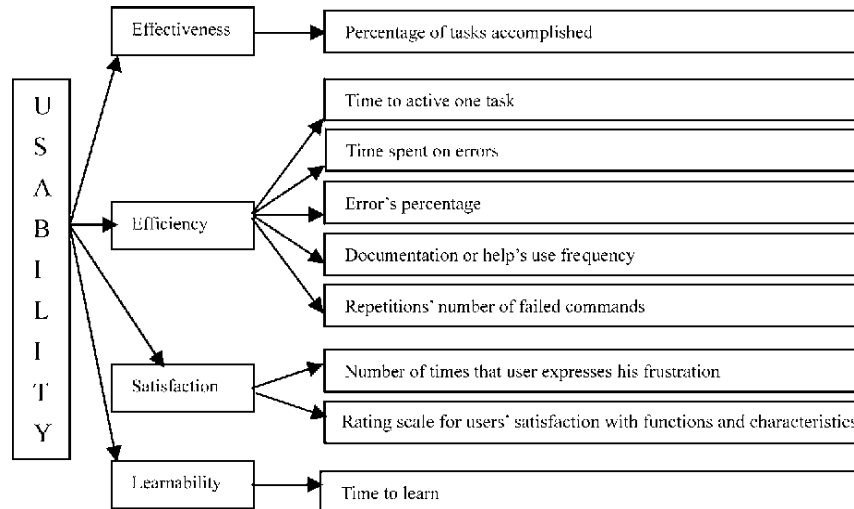


Figure 4.1: Detailed representation of usability characteristic, hierarchically organised from [105]

Finally, it is important to notice that *memorability* is a fundamental component for usability as previously discussed, although it is not properly an intrinsic feature of the system. No specific metrics for its measurement exists, unless evaluating the increase in performance in different-time-intervals test repetitions.

According to Seffah et al. [87], who examined existing usability measurement standards and models, 127 specific usability metrics can be identified. Depending on the development stage in which usability metrics are employed, two principal categories can be distinguished:

- *predictive metrics*, which can be referred to as design metrics, describe aspects of an estimate or prediction of usability in the initial development phase of the system;
- *testing metrics*, which permit to both analyse the system in use and detect problems, in the final development phase when a complete or a high-fidelity version of the system is available. The large amount of metrics of this category has implied a distinction between *preference metrics*, such as subjective evaluations, preferences and level of satisfaction, and *performance metrics*, such as success rate, error rate or completion time.

In this regard, in 1998, a list of possible evaluation measures has been published by usability specialists from Digital Equipment Corporation and IBM, subdivided into 6 sections [88]:

1. Counts of
 - commands used;
 - repetitions of failed commands;
 - runs of successes and of failures;
 - good and bad features recalled by users;
 - available commands not invoked/regressive behaviours;
 - users preferring the system.
2. Percentage of tasks completed in time period

3. Counts or percentages of
 - errors;
 - superior competitor products on a measure.
4. Ratios of
 - successes to failures;
 - favourable to unfavourable comments.
5. Times
 - to complete a task;
 - spent in errors;
 - spent using help or documentation.
6. Frequencies
 - of help and documentation use;
 - of interfaces misleading users;
 - users needing to work around a problem;
 - users disrupted from a work task;
 - users losing control of the system;
 - users expressing frustration or satisfaction.

Besides the arduous choice of metrics, an additional problem concerns thresholds, which has to be defined by each evaluation team, according to the evaluation objectives. Unfortunately, no assisting method currently exists for threshold determination.

A typical subdivision of metrics concerns *qualitative* and *quantitative* metrics, which reflect the distinction between preference and performance metrics:

- Qualitative metrics relate to non-numerical data, collected in general through questionnaires, regarding the subjective experience of the user with the system and as a consequence they are referred to as subjective metrics.
- Quantitative metrics refer to numerical values representative of the users' performance, acquired normally through automated tools and therefore addressed to as objective metrics.

To accomplish a comprehensive usability evaluation both types of metrics are necessary, considering the flaws each one presents. For example, subjective metrics can result not reliable as a consequence of the cognitive mediation and objective metrics rarely delineate satisfaction in a proper manner. In this regard, several physiological measures has been studied, based on the idea that they reproduce involuntary reactions of the autonomic nervous system providing a non-contaminated satisfaction information.

In the following sections, subjective and objective metrics are investigated in more detail.

Subjective metrics

Subjective reactions to the usability of a product or application illustrate users' behaviour and purchasing decisions procedure, which are nowadays fundamental to the success of a system. Nevertheless, frequently, performance measures are favoured to estimate usability, especially when a distinction between different products must be executed [106].

This category of metrics is often referred to as self-report measures. It relies on the subject perceived experience of the interaction with an underlying interactive system through the direct estimation of individual differences, such as the emotional state, attitude and stress, the effort devoted to the task and its demands [107].

In the beginning, the mainly importance of these type of metrics has been investigated by Ameritech, which anticipated the possibility to generate questionnaire in order to acquire users' impressions. Moreover, previously several studies in MIS (Management Information System) and technology diffusion areas have addressed both the relevance and the relationships between usefulness, satisfaction and ease of use in a system.

Thereafter, the majority of usability tests conclude with a questionnaire, based in general on a 5-point rating, addressing various characteristics of the system in order to evaluate the mental workload.

It is therefore important to emphasise the presence of response bias, which profoundly affect final results of these type of usability measurement. In fact, participants tend to respond inaccurately or falsely, depending on various characteristics of the questions. Choi et. al [108] identify 48 types of bias, including for example ambiguous and complex question composition or technical jargon and uncommon or vague word utilization.

Notwithstanding reported issues, questionnaires remain the principal means to estimate user satisfaction. During the years, indeed, an enormous number of questionnaires have been composed for usability evaluation, causing confusion about which assessment would be most suitable.

The most popular questionnaire are described below [109]:

- *NASA Task Load index (TLX)*

It is based on six different dimensions, each rated through a twenty-step bipolar scale. The dimensions include:

1. mental demand;
2. physical demand;
3. temporal demand;
4. performance;
5. effort;
6. frustration.

A second part of the questionnaire requires participants to compare pairwise the dimensions, according to the perceived importance, in order to obtain a weighting of the dimensions. For each rated task, a final score is calculated by multiplying the weight by the individual dimension scale score, summing across scales and dividing by the total number of paired comparisons, which is 15.

The Official NASA TLX is available in both paper and pencil version in PDF format and as mobile app on the App Store, in order to cope with the massive demand.

NASA TLX has been successfully employed worldwide in various environments, for example command, control and communication workstations, supervisory and process control and finally in simulations and laboratory tests. Moreover, it has been used for evaluating user interfaces in health-care [27] or in e-commerce [107].

- *Subjective Workload Assessment Technique (SWAT)*

It is based on three dimensions, further defined by a set of descriptors that specify three levels (i.e. low, medium, high) of each of the dimensions:

1. time load, which is “the availability of spare time and the overlap of task activities. Time Load may be experienced as the rate that events occur or the speed of a system.” [110].
The three levels are:
 - (a) “Often have spare time”, which indicates interruptions or overlap among activities that occur infrequently or not at all;
 - (b) “Occasionally have spare time”, which refers to frequently interruptions or overlap among activities;
 - (c) “Almost never have spare time”, which denotes remarkably frequent interruptions or overlap among activities.

2. mental effort load, which is “the amount of attention or mental demands that are required to accomplish a task, independent of the number of subtasks or time limitations. Generally, this is due to the complexity of the task or the amount of information which must be processed by the operator in order to perform adequately. Activities such as performing calculations, making decisions, remembering or storing information, and problem solving are all examples of mental effort.” [110].

The three levels are:

- (a) “Very little conscious mental effort or concentration required”, which indicates almost automatic operation, with no or little need for attention;
 - (b) “Moderate conscious mental effort or concentration required”, which indicates a moderately high complexity, due to uncertainty, unpredictability or unfamiliarity;
 - (c) “Extensive mental effort and concentration are necessary”, which indicates extremely complex operation requiring total attention.
3. psychological stress load, which “refers to conditions that produce confusion, frustration, and/or anxiety during task performance and, therefore, make task accomplishment seem more difficult.”

The three levels are:

- (a) “Little confusion, risk, frustration, or anxiety exists and can be easily accommodated”;
- (b) “Moderate stress due to confusion, frustration, or anxiety noticeably adds to workload”;
- (c) “High to very intense stress due to confusion, frustration, or anxiety”.

In order to calculate the degree of workload, a set of 27 cards, characterised by a capital letter and representing specific combination of the three levels, are provided to the participants. They are required to order the cards according to the personal perception of the workload, in ascending order. Subsequently, a scaling solution for the data is calculated and each three-dimension rating is converted into numeric scores between 0 and 100.

SWAT has been applied successfully in the mental workload assessment of several aircraft multitask conditions or nuclear plant simulations. simulators

- *Workload Profile (WP)*

It is a multidimensional instrument based on a multiple resource model, in which individuals are characterized by possessing different capacities (resources), concerning different dimensions.

The dimensions are:

1. stage of information processing, perceptual or central processing and response selection or execution;
2. code of information processing, spatial or verbal;
3. input, visual and auditory processing;
4. output, manual and speech output.

For each task, the participant is required to sign (enter 0 or 1) the corresponding dimension, in order to express the necessity of cognitive effort. Subsequently, the ratings on the individual dimensions are summed to provide an overall workload rating.

- *System Usability Scale (SUS)*

It is a 10-item Likert scale, with include five possible responses, from strongly agree to strongly disagree. SUS is widely used in industry, because of several advantages, such as the ability to provide reliable results on small sample sizes, the ease of utilization and its attested validity [111]. The 10 items are:

1. I think that I would like to use this system frequently;
2. I found the system unnecessarily complex;
3. I thought the system was easy to use;

4. I think that I would need the support of a technical person to be able to use this system;
5. I found the various functions in this system were well integrated;
6. I thought there was too much inconsistency in this system;
7. I would imagine that most people would learn to use this system very quickly;
8. I found the system very cumbersome to use;
9. I felt very confident using the system;
10. I needed to learn a lot of things before I could get going with this system.

Finally, by means of a complex mechanisms, summarizing each score, a value between 0 to 100 is calculated.

SUS is employed in hardware, software, mobile devices, websites and applications evaluations.

- *Post-Study System Usability Questionnaire (PSSUQ)*

It is a 19-item questionnaire, based on a 7-point scale, which present an additional N/A (Not Applicable) option, whose aim is to measure the overall users satisfaction of a system [112].

The factors addressed are:

1. quick completion of work;
2. ease of learning;
3. high-quality documentation and online information;
4. functional adequacy and rapid acquisition of usability experts and several different user groups.

An alternative to PSSUQ is CSUQ (Computer System Usability Questionnaire), which contains identical items, but an appropriate wording for use in field settings or surveys.

PSSUQ can be particularly useful in evaluating competitors or usability changes during the system development, for example within a version or between versions.

- *Questionnaire for User Interface Satisfaction (QUIS)*

It is a 21-item questionnaire, based on a 10-point scale, including the N/A (Not Applicable) option, measuring in particular interface factors. More precisely, 11 characteristics are addressed [113]:

1. screen factors;
2. terminology and system feedback;
3. learning factors;
4. system capabilities;
5. technical manuals;
6. on-line tutorials;
7. multimedia;
8. voice recognition;
9. virtual environments;
10. internet access;
11. software installation.

QUIS presents several advantages, such as ease of administration and adaptation to researchers needs and limited expertise or training require.

- *Software Usability Measurement Inventory (SUMI)*

It is a 50-item questionnaire, based an three possible responses, i.e. agree, don't know, disagree. On the contrary of previous schemes, the decision of a reduced set of reactions derives from an early version review, where participants complained regard the difficulty of discriminating through 5 or 7 different levels of satisfaction [114]. An advantage of this technique, in addition to the narrow timing, is the restricted number of users required to achieve a tolerable precision of the analysis. Nevertheless, the sample size is not crucial as

the context investigation and the design plan.
SUMI provides three different type of results:

- a global score, which refers to the overall subjective usability;
- a set of five subscales, which includes affect, efficiency, helpfulness, control and learnability;
- ICA (Item Consensual Analysis) for formative evaluation, permitting a more precisely identification of the usability problems.

SUMI has been employed in the MUSiC project and therefore by the industrial partners within the MUSiC consortium. The Human Factors Research Group have received by authors notice to recommend SUMI, indeed the latest draft of the ISO 9241 Part 11 references SUMI. It is available both as a paper-and-pen format and computerized version.

Objective metrics

The main issue of subjective metrics is the strongly influence of the human cognitive process, which distorts reality and therefore provide unreliable results.
For this reason, in general, software engineers are frustrated and sceptical about the subjective usability outcomes and therefore prefer to evaluate a system in basis of more consistent data, provided by objective measures of the performance of the user [115].

Objective metrics assess different aspects of the interaction between the user and the system, with the aim to not involve the individual perception of the person. These measures regard two specific components of usability, i.e effectiveness and efficiency, and are obtained normally measuring several characteristics of a set of tasks imparted to the user.

As previously discussed, objective metrics regard quantitative performance values, such as the success rate or the task completion rate, the error rate, several time or failure related rates. As a consequence, several tools has been developed in order to analyse the users' performance. The majority of these tools are automated mechanisms (see 4.2.1), which permit the acquisition of a massive amount of data and a rapid and comprehensive analysis of the system [116].

According to the study of Hornaek [116], who has examined 180 different studies from the HCI research literature, the main metrics for evaluating effectiveness and efficiency of a system can be summarised in the following definitions.

For effectiveness, the review indicated:

- *binary task completion*, which refers to the completion or not of a task and includes several different measures, such as the number of correct tasks, the number of fail tasks, either for timeout expiration or waiver by the user.
- *accuracy*, which refers to the accuracy of the completion of tasks and therefore it can be represented by error rates. It can include for example the number of errors in data entry or the number of hints given by the experimenter. In addition, two subgroups of accuracy are indicated:
 - *spatial accuracy*, a typical measure of input devices studies and refers to “the accuracy in pointing to or manipulating user interface objects”;
 - *precision*, a typical measure of information retrieval systems, which refers to the ratio of the correct number out of the total number of documents retrieved.
- *recall*, which refers to the amount of information that a user can recall after the interaction with the interface. In particular, it is considered information parts of the content of the interface, such as the banner ads and their implementation.

- *completeness*, which considers users' extent to task completion. It does not refer to users' errors, instead, it represent the degree of completeness of a solution. For example, it includes the number of secondary tasks solved and the proportion of relevant documents found in information retrieval tasks.
- *other measures*, which represent users' ability to predict the functioning of the interface and changes in users' health.

A similar analysis has been conducted on efficiency. The principal metrics identified are:

- *time*, which is the time required by users to complete tasks with the interface. In addition, various studies collect time information according to the nature of the interaction, such as time spent in the help function or in the dialogue boxes, and time elapsed before a certain event.
- *input rate*, which represents in general the text entry speed (e.g. words per minute, corrected words per minute) or throughput.
- *mental effort*, which refers to the mental resources users spend on interaction.
- *usage patterns*, which represent the usage of the interface by the user, with the purpose to determinate the resources expended in the task solution. Three different kind of usage pattern have been recognised:
 - the number of times a certain action has been performed, for example the number of keystrokes or mouse clicks;
 - the amount of information users access when solving tasks, for example the number of objects visited in a virtual space;
 - the deviation from the optimal efficient solution, which refers for example to the ratio of actual distance travelled to shortest distance in travelling information spaces and the number of target re-entries in the target area.
- *learning measures*, which are typically represented by alterations of efficiency of the interface usage. They include, for example, the completion task time or enhancements in text input over time.

Regarding the usability component of satisfaction, a first attempt to obtain objective measure of this characteristic is calculating the mental effort. Although, currently, the prominent practice in satisfaction evaluations consider subjective questionnaires the most convenient mean, researchers investigate new techniques to acquire data of individuals' contentment in a reliable manner.

In this context, physiological measures has been examined in view of the fact that, as previously mentioned, they reflect involuntary reactions of the autonomic nervous system. Indeed, throughout the years, physiological measures have been employed as objective identifiers of human emotions, such as anger, grief, sadness and stress. As a matter of fact, according to Lin et al. [117], "physiological measures are consistent with subjective measures and show significant sensitivity to changes in stress levels.". Furthermore, although it is arduous to elucidate the cause-effect relationship, a correlation has been found between task performance and physiological data.

The main advantage of these type of metrics is the complete absence of any explicit response by the user, who can be monitored continuously during the evaluation. Nonetheless, on the other hand, physiological measures necessitate specific equipment and trained operators, causing hindrance in employability in real-world assessment. Fortunately, the progress in sensor-based technologies to monitor physiological signals is reversing this tendency.

According to Lin et al. [117], the importance of the exploitation of physiological measures, in order to obtain information of individual satisfaction of a system, is evident in a study regarding multimedia quality in the context of networked applications. The subjects, despite not having reported any annoyance in watching two videos at different resolutions, experienced a consistently increase in both their levels of GSR (Galvanic Skin Response) and HR (Heart Rate).

Typical metrics include brain function measures, cardiac measures (e.g. heart rate, galvanic skin response, blood volume pulse), eye measures (e.g. pupil dilation or movement) and muscle measures. In particular, the majority of the studies involve the following metrics:

- *Electroencephalography - EEG*

Several neurological studies have shown the relationship between brain waves and human emotions and it has been exploited in various studies on usability [118]. The participants are required to wear EEG scanner, typically on their head and performs the selected tasks. The brain activities are collected and further analysed, in general through the frequency domain, assigning different emotions to distinct range of frequencies. For example, alpha waves (approximately 7.5 - 14 Hz) are associated to relaxation and calmness, while beta waves (approximately 14 - 40 Hz) represent attentive brain work and severe beta waves could indicate stress, loneliness and restlessness. Nevertheless, a large number of samples are necessary to generalize the results. Nowadays, as a consequence of technological advances of hardware devices, the effort is to product mobile EEG systems, in order to address the principal issues of EEG, such as intrusiveness and costs.

- *Functional Near Infrared Spectroscopy - fNIRs*

Introduced in the 1990s as an enhancement to EEG, fNIRs is a tool based on light sources, in the near infrared wavelength range, which provides an accurate measure of activity within the frontal lobe of the brain. In fact, it has been stated that frontal lobe affects memory and executive control. The principal characteristics of fNIRs are safety, portability, minor invasiveness and moreover, the possibility of wireless implementation, which permits the employment in real world environments [120].

- *Galvanic Skin Response - GSR*

It refers to the electrodermal activity of the human body, which alters the skin conductance on the basis of psychological or physiological arousal. In general, skin conductance is related to the variation of the state of sweat glands in the skin, whose activity increase in case of stimulation of the autonomic nervous system⁸, resulting in an increment of skin conductance [117]. It is important to notice that only the alteration from the relaxed state is collected and the elicited specific emotion is not delineated. Nevertheless, GSR variations are typically associated with stress, fatigue or involvement. The skin conductance information is collected, at least, through two electrodes applied to the index and middle fingers of one hand. The massive intrusiveness of the necessary equipment has lead to the creation of new wearable and fashionable commercial devices, such as bracelets or watches, enabling neuroscience studies in any experimental condition, also different from laboratory. There has been a notable increased interest in recent years in using GSR as an objective measure of usability in HCI, as mentioned in [117].

- *Heart Rate - HR*

It has been the most practical and popular mechanism to asses mental workload, reflecting positive or negative emotions, by means of finger temperature. Nevertheless, throughout the years, HR has been recognised as a part of the complex homeostatic cardiovascular system, which include several processes (i.e. energetic, thermoregulatory, respiratory, emotional and cognitive processes) and therefore neglected in favour of HRV, result of the attempt to decompose the processes which influence cardiovascular regulation [119].

- *Heart Rate Variability- HRV*

It is based on the oscillation of the interval between consecutive heartbeats, principally stimulated by sympathetic nervous system⁹. In fact, in case of physical or psychological

⁸The addressed “sweat glands” are eccrine glands, located in the palms and feet, which respond to psychological stimulation rather than a common temperature variation [119].

⁹“A part of the nervous system that serves to accelerate the heart rate, constrict blood vessels, and raise blood pressure. The sympathetic nervous system and the parasympathetic nervous system constitute the autonomic nervous system.” from MedicineNet (<https://www.medicinenet.com/script/main/art.asp?articlekey=5607>).

stress, the SNS activity prevails, causing physiological arousal [121].

In general, a high level of heart rate variability represents calm state, minor levels of anxiety, distress and a regulated emotional responding. On the contrary, a reduced HRV indicates emotional dysregulation, such as anxiety, depression or rigid attentional processing of threat. The heart beat trace is acquired through an electrocardiogram, which requires commonly 10 electrodes to be placed on each of the four limbs and at different locations on the anterior surface of the chest. The majority of the studies adopting both HR and HRV to usability measurements concern games usability evaluation [122].

- *Eye-tracking*

It represents the most popular and historically employed physiological metric, and consists in identifying the most targeted regions of an interface, through the individuals' movement of the eyes. It has been employed in studies since the 1950s, affecting deeply researchers, especially during the 1970s, when the impact of the human eye movements on perceptual and cognitive processes prevailed against the mere utilization for efficiency evaluation. According to Jacob et. al [123], who review 21 different usability studies, 3 different components are the most assessed:

1. fixation, which refers to a stable position of the eye (pupil) within a dispersion threshold (approximately 2°) for a minimum amount of time, typically from 100 to 200 ms, and a certain velocity, generally imposed as 15-100 degrees per second);
2. gaze duration, which represent the “cumulative duration and average spatial location of a series of consecutive fixations within an area of interest”, and terminate in the case a fixation exit the area of interest;
3. scan path, which is the “spatial arrangement of a sequence of fixations”.

Although they have been considered particularly challenging, diverse aspects of ocular-motor performance can be exploited to obtain elaborate evaluations, for example blinks, pupil changes, convergence or accommodation. In general, the results of eye-tracking are generated in the form of heat maps and saccade pathways (Fig. 4.2).

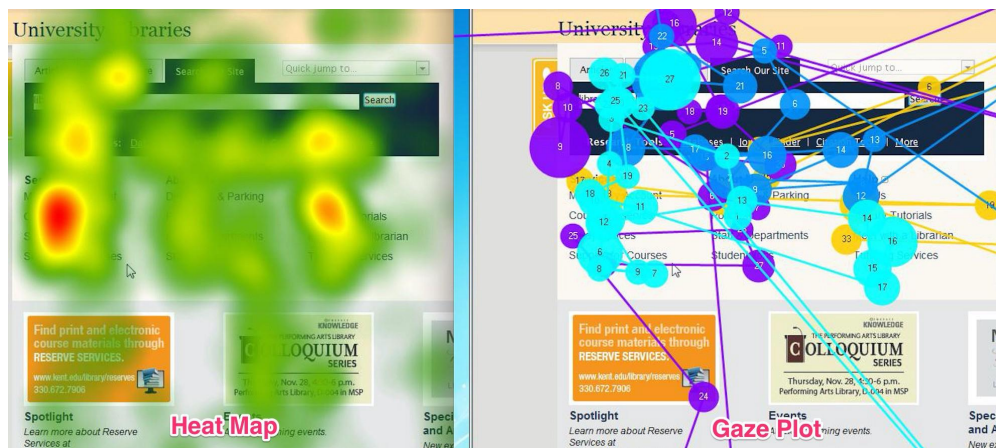


Figure 4.2: Heat map and gaze plot examples from [173]

It is important to specify that this type of metric presents various limitations, besides the common disadvantage of the physiological measures of distinguishing positive or negative perception. Indeed, difficulties has been found with participants having small pupils or wandering eye, or wearing glasses or hard contacts. Moreover, it is common behaviour to unintentionally point an area for a short period of time.

- *Electromyography - EMG*

It represents the muscle activity of a particular area of the human body, detecting surface voltages of a contracted muscle. In general, for usability evaluations, the electrodes are placed on the jaw, in order to measure tension more precisely or on the face, permitting to discern between positive and negative emotions, according to the frown and smile muscles' movements. Several factors, including the dimensions of each electrode (approximately 5 mm) and the position around mimic muscles, produce complexity in the application and frustration for the users. Furthermore, signals from electrodes can be contaminated by different facial muscle activity (e.g. talking) and therefore, needles has been proposed as alternative to surface electrodes, in order to minimize interference [122].

It has to be noticed that mental workload is a peculiar characteristic to be measured related to usability, because the nature of the strain caused remains uncertain. In fact, high levels of workload could indicate not necessarily an unsatisfactory experience, but it could reveal high concentration and involvement in the task solution. Indeed, some researchers prefer to distinguish stress into "eustress" and "distress", which represent respectively the positive and the negative connotations of stress.

In conclusion, notwithstanding the massive contribution of physiological metrics in the area of usability evaluation, providing reliable and unbiased outcomes, they must be complemented with other preferably subjective metrics, in order to be able to determinate the actual perception of the user.

4.5 Usability evaluation of authentication methods

The introduced usability methodologies and metrics reveal the possible problems encountered by the users during the interaction with the system and they can be effectively employed in the evaluation of authentication systems as presented.

Nevertheless, in the particular case of authentication, it is fundamental a proper evaluation approach, which consider both usability and security, in order to perform an adequate analysis and provide the most secure and suitable system to satisfy the users' needs.

Furthermore, the absence of a standardisation regarding usability techniques and measures represent a challenging obstacle to the evaluation of a system, which is typically analysed in a unique manner, causing an impracticable concrete comparison [124].

Although numerous studies in the literature assess the usability of specific authentication mechanisms, a scarce number of researches investigate the different aspects to be considered during the evaluation of an authentication system, in the attempt to balance usability and security. Moreover, in the same manner, the majority of these studies refer to definite authentication categories, such as biometrics or tokens.

In this regard, Mihaĳlov et. al [124] propose, in its quantification approach, aimed to concurrently evaluating the security and usability factors of a system, 5 security characteristics and 5 usability criteria to examine during the evaluation of an authentication system.

Respectively, the first regarding security are:

1. secrecy, which refers to unpredictability of the secret, based on random properties;
2. abundance, which refers to the authentication key space, which directly influences breakability, because a vast space increases the time required to compromise the key;
3. revelation, which refers to the disclosure of the secret, from both users and the system;
4. privacy, which refers to the presence of private or sensible information, required by the authentication mechanism;
5. breakability, which refers to the effort needed to access the systems or the algorithm which generates the authentication key (i.e. exposition to attacks, such as research, brute-force, dictionary and keylogging attacks).

On the other hand, regarding usability are indicated:

1. meaningful retrieval, which refers to the mental effort required to retrieve and deduce the authentication key;
2. processing depth, which refers to the cognitive activity involved in the encoding of an authentication secret (e.g. cognitive, rehearsal, visual);
3. requirements, which refers to the specification of the types of resources needed for the authentication mechanisms (i.e. hardware, software, technical expertise);
4. convenience, which refers to the consumption of time during the enrolment, authentication and replacement processes;
5. inclusivity, which refers to the property of the system to be accessible to everyone, regardless cognitive, mobility or sensory disabilities.

In addition to the aforementioned factors, more detailed objective indicators are commonly employed, following the usability-deployability-security (UDS) scheme presented by Bonneau et. al [125], where twenty-five characteristics of the ideal authentication system are involved (4.1).

Usability	Deployability	Security
Memorywise-Effortless		Resilient-to-Physical-Observation
Scalable-for-Users	Accessible	Resilient-to-Targeted-Impersonation
Nothing-to-Carry	Negligible-Cost-per-User	Resilient-to-Throttled-Guessing
Physically-Effortless	Server-Compatible	Resilient-to-Unthrottled-Guessing
Easy-to-Learn	Browser-Compatible	Resilient-to-Internal-Observation
Efficient-to-Use	Mature	Resilient-to-Leaks-from-Other-Verifiers
Infrequent-Errors	Non-Proprietary	Resilient-to-Phishing
Easy-Recovery-from-Loss		Resilient-to-Theft
		No-Trusted-Third-Party
		Requiring-Explicit-Consent
		Unlinkable

Table 4.1: Benefits of the ideal authentication system

Furthermore, a comprehensive study based on both objective features, such as the previously mentioned, and subjective users' perceptions was conducted reviewing different categories of authentication (i.e. text password, graphical password, cognitive, biometric, token) by Zimmermann et. al [126], evidencing the necessity to include subjective metrics to the evaluation of the system. In fact, the results suggest a deviation from the actual objective evaluation (based on Bonneau's features) of the authentication schemes from their actual perception, considering that in general people tend to prefer usable systems, which provide an illusory security.

In the following sections, specific observations on the usability advantages and disadvantages of the authentication systems are analysed in more detail.

4.5.1 Alphanumeric passwords

Alphanumeric passwords represent the most popular authentication mechanism currently utilized worldwide in various environment. The ease of use derived from the intuitive operations and the users' familiarity with this mechanism permits to accomplish the authentication procedure rapidly and with minor errors.

In this regard, the most common errors concern typing wrong characters, resulting in failed authentication and frustration for the user. In order to overcome this type of errors, a clear input in the prompt, instead of a masked password, could be implemented.

On the other hand, as a consequence, the security level of the entire system is compromised, facilitating an attacker to steal the password. A solution could be represented by a recovery

method in case of typographical error.

Furthermore, in some cases several logins are required in order to avoid attackers to remain logged on, in case of successful intrusion, with the solely result of incrementing user's distraction, disappointment and reluctance [163].

The principal concern of passwords regards the users' inability to create robust and memorable passwords, satisfying the restrict policies imposed by each system. In the Kumar's survey [127] emerged that the 85% of the 202 participants usually inserts digits within the generated password, but only the 40% introduce a capital letter and/or a special character. Furthermore, it has been evinced that the majority of the participants draw inspiration from family members' names or numbers and from favourite celebrities, constructing easy hacking, cracking and guessing passwords. As a consequence proactive password checking has been introduced, controlling adherence to constraints.

Related to this background, system-generated passwords has been adopted, profoundly affecting memorability and user's contentment. Nevertheless, according to the survey, which include principally academic members, the 33% is unaware of the existence of computer program able to create passwords and a total of 62% does not utilize any, indicating a high level of scepticism about these mechanisms.

Notwithstanding the difficulties of the single password, a major problem concerns the multitude of passwords each user has to remember and maintain. According to the survey, indeed, the 60% of the participants possesses at least 6 different password, including web sites, emails and computers and the 70% reuse them. Moreover, the 67% does not change passwords, neither in general nor annually. As a consequence, the majority of participants can recall passwords solely exploiting their memory, whereas a conspicuous number of subjects admitted to store them on computer unencrypted files or writing them down on paper.

In conclusion, in conformity with the Bonneau's characteristics [125], passwords are not Memorywise-Effortless nor Scalable-for-Users, in fact different passwords must be generated, following specific requirements and guidelines, for each system to authenticate to. Although they are characterised by the Nothing-to-Carry benefit and therefore Resilient-to-Theft, they cannot be held Physically-Effortless, due to the input necessity, which represents the main source of errors, and therefore they present Quasi-Infrequent-Errors. In general alphanumeric password usability is considered extremely adequate, considering that they are Easy-to-Learn and Efficient-to-Use, in addition to provided of Easy-Recovery-from-Loss.

On the contrary, though, alphanumeric passwords result seriously scarce concerning security. Indeed, they result not Resilient-to-Physical-Observation nor Resilient-to-Internal Observation, furthermore they are not Resilient-to-Leaks-from-Other-Verifiers, Resilient-to Phishing.

4.5.2 Graphical passwords

The security problems which characterise passwords have induced the investigation of new authentication systems, more secure and usable. Indeed, graphical passwords are renowned both for considerable memorability and ease of use.

Nevertheless, they result time-consuming not only during the registration process, but also during the login phase, considering that typically the user is requested to select the pass images (or points) from a set predefined pictures. Consequently, the procedure is perceived tedious and complex.

In this context, it has been proven that user-chosen graphical passwords, although they produce a more usable system increasing memorability, are predictable at the same level of alphanumeric passwords (e.g. DAS, PassPoint and Passfaces suffer from predictability).

Furthermore, users tend to select similar meaningful images, which can create the "interference effect", which reflects the human tendency to remember comparable but not exactly equal images, and therefore causes confusion over the multitude of accounts and frustration in failing authentication. A solution is to assign randomly selected graphics to each user, which implicate a massive amount of time for training individuals to remember the designated secret. In addition,

the interference effect must be taken into consideration even in this case, in order to not mislead the users [17].

Therefore, timing represents a crucial issue of graphical authentication systems, as it additionally affects the application in several use cases, such as frequently accessed systems (e.g. social media), which necessitate a rapid and simple authentication mechanism.

Moreover, the size and the resolution of the images, which heavily affect usability, preclude the use of different devices, functionally inadequate for this type of authentication.

In addition, an important feature to consider in graphical systems is the grid provided, both to draw or select images as discussed in [128]. In fact, Balk et al. propose interesting hypotheses regarding the correlation between the size of the grid presented to the user, and security and usability properties. Although their study is focused on recognition-based graphical mechanisms, the mentioned assumptions can be generalised for any type of grid displayed. From the perspective of security, increasing the amount of image alternatives (and therefore the key space) is a granted countermeasure against password hijacking attacks. However, in the study it has been observed that a certain threshold must not be exceeded, in order to deteriorate usability, potentially nullifying the benefits introduced by these techniques. In the particular case of recognition-based mechanisms, results of the research has revealed that a grid of 60 to 90 images is the usable in terms of graphical login, demonstrating that 30-images grids cause the generation of inadequate graphical passwords, meaningless and hardly memorable, furthermore resulting in increasing timing.

Another issue essential to emphasize is the extensive load needed to store and transfer the significant amount of images required by this mechanisms, which in case of worldwide application can lead to an overload of the network, providing the user with poor service.

Finally, the graphical authentication systems exclude users with vision complications, colour-blindness and even motor disabilities at any level, resulting not accessible to a large part of the population.

According to Bonneau's analysis of graphical authentication systems [125], who in particular evaluated two specific mechanisms (i.e. PCCP and GrIDSure, presented in subsec:cuedrecall and subsec:purelyrecall), some general considerations can be deduced. Purely recalled-based schemes are comparable to alphanumeric passwords in terms of usability, excepting for the Efficient-to-Use benefit, which in this case is reduced to Quasi-Efficient-to-Use, due to the cognitive and timing effort derived from the direct interaction with the grid cells.

Cued recall-based systems, as well as purely recall-based and alphanumeric passwords, are neither Memorywise-Effortless, nor Scalable-for-Users, but Easy-to-Learn. Further, they are considered Quasi-Efficient-to-Use, due to timing, and presented in best-case scenario as Quasi-Infrequent-Errors. Along with purely recalled-based techniques, they are considered not Accessible, considering physical constraints required, and have Negligible-Cost-per-User.

Moreover, both the schemes are neither Resilient-to-Physical-Observation, nor Resilient-to-Unthrottled-Guessing nor Resilient-to-Internal-Observation. While pure recalled systems are completely Resilient-to-Throttled-Guessing, cued systems are considered Quasi-Resilient-to-Throttled-Guessing, as a result of the systemic persuasion which improves password randomness. Furthermore, they are Resilient-to-Leaks-from-Other-Verifiers and Resilient-to-Phishing. Finally, both the mechanisms are Resilient-to-Targeted-Impersonation, considering arduous for an attacker to discover the secret knowing the user.

A specific study on recognition-based graphical authentication systems has been conducted by Khodadadi et al. [], identifying 9 major usability features to consider in an evaluation, which are User assigned Images, Meaningful Images, Category of Images, Easy and Fun to Use, Easy to Create, Easy to Execute, Easy to learn and Understand, Easy to Correct, and Nice and Simple Interface. The results prove that, although several systems are resistant or immune to existing attacks (e.g. shoulder-surfing attack), they present significant usability drawbacks, in particular concerning slow login times and memorability, requiring a more effort in order to adequate to security measures.

4.5.3 Token

In the same manner of other additional authentication methods, the utilisation of tokens (e.g. smart cards or USB) improves authentication security, providing a second factor for authentication, at the expense of some limitations.

The principal disadvantage concerns the additional financial costs associated with procuring, implementing and maintaining both required hardware and software for the mechanism.

Furthermore, in general, hardware tokens are small-size tamper-resistant modules carried by the user and therefore one of the most common drawback associated to them is loss or theft, in addition to the physical burden of constantly carry them. As a result, users typically experience both anxiety about the risk and anticipated annoyance associated with the possible inconvenience [129].

Different types of token exist with specific usability disadvantages. For instance, disconnected tokens display the OTP for a limited time and the user must introduce the password before it expires, providing eventually stress and frustration in entering the correct input promptly. On the other hand, contact tokens require the user to insert the hardware into a reader, which typically result in wrong entry.

Regarding the acceptability of tokens as authentication mechanism, an interesting study has been conducted on 141 participants by Weir et al. [130], comparing the usability of three different hardware tokens in a financial environment. The results stated that users tend to prefer the most perceived usable token, regardless of the level of security provided, which in a financial scenario should be the primary factor.

Conclusive evidence of the scarce acceptance of tokens for personal use can be commonly deduced from the outcomes of several studies in the literature, which demonstrate the users' propensity to employ tokens in work or banking contexts.

Another more specific study on USB tokens conducted by Das et al. [131], addressed the usability and adoption issues associated to Two-Factor Authentication with the Yubico FIDO U2F security key. The results demonstrate the profoundly unfamiliarity of the participants with this type of mechanism. The two-phases experiment proved that an increase of the level of detail in the information provided to the user for the usage of the tokens extremely increases usability. Nevertheless, a major number of participants admitted to continued to believe in the superiority of passwords over the proposed mechanism.

4.5.4 Biometric authentication

Traditional authentication systems rely on properties that can be forgotten, disclosed, lost or stolen. The main strength of biometric systems is that the physical or behavioural characteristics of a human being are, or at least should be, unique and not duplicable or transferable.

Although the use of each biometric technology has its own specific issues, the basic operation of any biometric system is very similar, permitting a collective summarisation of the most influencing usability drawbacks [132].

In first instance, a biometric sample must be acquired through a specific device, which differ in size and intrusiveness, in base of the biometric mechanism utilised. A proper technologically-advanced instrument is fundamental in order to both generate a biometric sample of sufficient quality and reduce the number of sample acquisitions, in the interest of not bother the users. In addition, in several cases, the users are unfamiliar with the acquisition method or technology, necessitating a guidance through the sample collection and therefore the entire system is perceived as time-consuming and not intuitive.

Moreover, the involvement of an biometric input device raise a crucial issue, which concerns the reliability of the instrument. In fact, its authenticity should be verified to provide a physically and digital secure transmission of the acquisition. Therefore, it is important to submit the device to a human supervision or validate its tamper-resistance. Furthermore, several biometric sensors have a limited lifetime, due to physical contact with users and in particular scenarios, such as

in companies, they can resist no more than a year (magnetic card readers may resist years or decades).

Nowadays, the ubiquity of mobile phones, which are continuously more technologically sophisticated, has extended the idea of internally including several biometric methods. Although, fingerprints or face recognition techniques are currently popular, various hardware, computational capability and electricity power limitations exist, hindering the possible implementation of other biometric systems. Furthermore, concerning mobile devices, it is important to intensely analyse the security factors of this type of implementations, considering the openness of mobile communication signals, which produce an easy mean of attack.

The multitude of samples obtained is typically processed in order to create a “master template”, to which compare characteristics during the login phase. In fact, during this stage the real time acquisition has to match the composed template beyond a certain threshold. Based on this mechanism of comparison, according to the values in [132], equal error rates (EER) in general do not exceed the 1%, providing a false impression of accuracy of these systems. In fact, the false rejection rate (FRR) is rather high, approximately around the 10% in real applications, strongly affecting usability. In addition, a large number of biometric systems suffer from an elevated false acceptance rate (FAR), which is not tolerable in terms of authentication security.

It is necessary to state that sensitivity to errors is a design decision, dictated by the restriction imposed by the system. Indeed, some implementations require an elevated number of false negatives in order to be more prohibitive on user accesses. Although it compromises usability, the occasionally increase the threshold of legitimate users incorrectly rejected by the system is necessary depending on the security context [127].

Furthermore, it is evident that biometric authentication exclude part of the population with different deformities, such as injured eyes or missing fingers or even hands. In addition, peculiarities of a person can vary over time or be temporary damaged (e.g. cuts, burns, or blisters on finger), causing a fail to enrol. Besides the physical characteristics, it is essential to mention that user psychological state can be crucial to success of the authentication. In fact an alteration from the normal status, such as dilation of the pupil, hoarseness or sweat, can deviate the acquisition of the sample and preclude access.

It is important to notice that biometric characteristics are sensitive data that may contain a lot of personal information, resulting in a possible violation of the individual’s privacy. As a matter of fact, users as well as administrators and system engineers tend to overestimate security properties of biometric systems, proposing these mechanisms as alternatives to traditional authentication without a detailed and comprehensive risk analysis.

Nevertheless, frequently, biometric systems are considerate intrusive or personally invasive, resulting in a slightly sceptical acceptance. In this context, according to [133], cross-cultural (e.g. between United Kingdom, India and South Africa and even Saudi Arabia) surveys, regarding user acceptance of biometrics proved that acceptance is directly correlated with culture.

Notwithstanding exceptional cases, biometric peculiarities are mostly permanent and neither changeable nor exchangeable between users, especially in an easy manner. Biometrics, indeed, cannot be physically robbed as tokens, keys or cards, but in some cases it is possible to steal them from computer systems and networks. Nevertheless, in [133] is stressed to be careful about the utilisation of dead or artificial biometric characteristics.

The improbability to be stolen reduces problems and costs associated with lost, which is a major advantage for system administrators, saving some costs of the system management.

A comprehensive study on biometrics authentication schemes has been conducted by Z. Rui and Z. Yan [53], based on five criteria (i.e. accuracy, efficiency, usability, security and privacy), defined by different features (e.g. accuracy is determined by FAR, FRR and EER). Each biometric system has been analysed and successively insert into a category, which include face recognition, iris recognition, fingerprint or palm recognition, electrocardiographic signals, voice recognition and keystroke or touch dynamics mechanisms. A score range was therefore assigned for each

criterion, represented by high, medium and low values.

More specifically the results of the study demonstrate that fingerprint-based authentication mechanisms are in general currently widely employed, in several environment, providing a respectable accuracy and elevated efficiency (times around the millisecond). In addition, iris recognition proved to possess an excellent recognition accuracy and a minor error rate. Nevertheless, this technique has result to be typically considered intrusive and expensive, considering the supplementary equipment support required. Finally the study stated that the different discussed biometric authentication methods necessitate a further investigation, because considered still immature. In particular, authentication systems based on dynamic features (i.e. behavioural methods) demonstrate inferior accuracy and acceptance, in addition to higher costs related to auxiliary equipment. Nevertheless, further investigation is necessary, considering that these type of biometrics are extremely usable and adequately secure, representing a real potential alternative to traditional authentication

4.6 Conclusion

As usability testing becomes more and more a part of the life-cycle of software, particularly for web-based applications, it will be more and more important that testing methods are efficient, effective, inexpensive, and easy to use. Consequently, continual development of new methods is important to move from expensive, labour intensive methods to inexpensive, automated methods while maintaining a high level of diagnostics.

Chapter 5

Usage scenarios

In this chapter different use case scenarios are presented, with the aim to define the functional scope of the system to be developed.

In order to present the use cases, *time* has been assumed as a crucial characteristic, in consideration of the possible frustration caused by the prolonged times derived from the use of a graphic authentication system, with an extended training phase derived by the exploitation of the implicit memory effect. In fact, in the modern society, time is a fundamental resource that cannot be wasted and the perception of wasting time is one of the first causes of frustration. Nowadays, there is a general inability to wait, debilitated by the constant restlessness of being productive and therefore spend more time in a daily activity, such as authentication, can become a source of anxiety, stress and frustration.

As previously mentioned, graphical authentication mechanisms have been proven to be more secure than traditional passwords, although they have the main disadvantage of extending authentication times. In this context, use cases in which a greater expenditure of time can be tolerated (e.g. access to sensitive data) have been investigated.

Each use case is described by the following elements:

- *actor*, which indicates the individual or a group of individuals who interacts with the system;
- *objective*, which represents the final goal;
- *system*, which includes any mechanism useful to the user to achieve the goal;
- *pre-conditions*, which represents the verified conditions which permit to solve the task;
- *main success scenario*, which is the description of the interactions between the system and the actor (typically a numbered list of steps);
- *extensions*, which present the possible problems which can occur during the completion of the task;
- *improvements*, which include considerations about usability and security issues in order to enhance the use case.

5.1 #1: Company profile

Nowadays work is gradually detaching from traditional fixed workplaces, such as the office, as a result of the increasing improvements of technological connectivity, which offering the opportunity for the employees to work from anywhere and at any moment. According to Office for National Statistics, in 2014, the 14% of the employed in the United Kingdom spent at least half of their time working at, from or on the same grounds and buildings of their home. Moreover, an increase in the percentages of remote working can be seen globally, from United States to Europe.

The benefits concern both employees and employers, since the latter gain a more productive

workforce, which utilise less space and is more cost-effective. On the other hand, workers can obtain a better work-life balance, thereby increasing levels of job satisfaction and organisational commitment [134].

In this context, the remote user requires that any information accessed remain confidential. In fact, an unsecure communication link established between the remote location and the home office could allow third parties to intercept and read any transmitted data.

A common easy-to-use, cost-effective solution, which provides both authentication and encryption security measures is a Virtual Private Network (VPN).

Authentication is a prime concern in the process of connecting remote access users, involving a machine-level authentication (i.e. exchange of machine-level digital certificates during the establishment of a tunnel) and a password-level authentication (i.e. a user insert into a login prompt a login ID and a password). In order to increase its security an enhanced authentication mechanism is necessary to legitimate remote users, since the most popular systems rely on passwords, with the associated notorious drawbacks.

The case scenario is characterised by:

Actor An employee, who wants to access the company's data stored in the corporate or branch offices network.

Objective Successfully complete the transfer of reserved company data in a confidential manner and prevent any illegitimacy.

System The system is composed by the remote user's device with a desktop software installed, the dedicated hardware and servers for the VPN technology, in addition to a firewall at the VPN (Fig. 5.1).

Pre-conditions The employee must possess a secure trusted device with Internet access and a browser which imposes a TLS connection. Moreover, the employee must have installed a VPN technology and program into the company device. Finally, the employee must be registered and in possession of own valid credentials. The credentials are directly provided by the company, whose IT group configured the VPN.

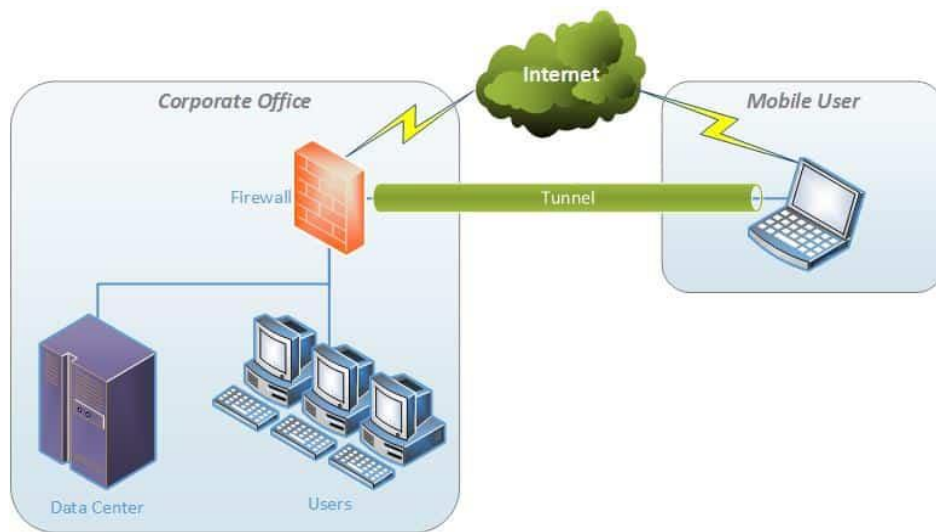


Figure 5.1: General VPN architecture from [135]

Main success scenario The interaction consists of the following steps:

1. The actor has to open the VPN program installed on the company PC and insert the valid credentials. If one of the credentials is incorrect, the access is denied.
2. Remote Access VPN realises a virtual network cable from the remote device to the LAN, through a negotiation process to build a secure VPN tunnel (e.g. involving encryption schemes and methods to be adopted).
3. The employee's device is now seen as being on the same local network as your VPN and therefore in practical terms it can exchange encrypted communication with the remote gateway.
4. The client can access remotely any applications for LAN-oriented, such as groupware, SAP, SQL client and enterprise systems, and request the wanted data.
5. Data from the company network travels through the secure VPN tunnel over the Internet and reaches the remote user.

Extensions In first instance, the VPN end-points devices can present vulnerabilities, causing serious security breaches and essentially invalidating the final objective of confidentiality. In fact, the corporate network side of the VPN can be protected by a firewall, but the mobile user or remote client location needs to implement proper own protection. For example, the presence of a virus or spyware, infecting a client machine, can allow the leakage of the authentication secret to an attacker.

Furthermore, if the VPN client machine is compromised, either before or during the connection, it exposes the connecting network to risks.

In case of insecure authentication credential storage, the risk of a successful attack remains, especially if significant computational resources are available on the adversary side. It can occur that the VPN is not configured properly, permitting IP and DNS leaks, which turn private data vulnerable to hackers and other online threats. Moreover, even if strong cryptographic algorithms are applied, DoS attacks can prevent communications. In addition, the insertion of employee credentials during the configuration of the VPN, which is IT technicians' responsibility, can be highly subject to human errors and therefore result in a potential source of danger.

Finally, the VPN technology utilized can affect the performance of the network.

Improvements The company, which provides the remote devices, should implement complementary preferred security measures, such as personal firewalls, malware scanning, intrusion prevention, OS authentication and file encryption.

Furthermore, considering that a VPN with a limited number of users connected is more secure, the amount of devices should remain restricted.

VPN vendors should include additional security measures into the client software, allowing the organization to eventually pre-configure them prior to installation.

The user-based authentication mechanism imposed should be memorable and usable, in order to not add obstacles to the employees, who already have several company authentication secrets to know. Furthermore, a system-assigned authentication mechanism represents a solution to associate a robust and policy-compliant secret to each employee, in order to overcome the human-factor issue, besides the insertion of the respective employee's credentials during the configuration of the VPN.

In addition, an improvement should be made in the interoperability of the VPN technologies, in order to enhance flexibility.

In conclusion, in a working environment, the confidentiality of data is essential. If an attacker obtains employee's credentials, the entire business system could be endangered. For this reason, it is fundamental to implement an authentication mechanism that relieves the worker from managing them. In fact, particularly in this context, in which credentials are provided by technician figures, the risk of being written down and kept in an unsecure manner increases significantly. Moreover,

the fact that they are associated with the employee and not personally created does not imply that they are not connected to something which can represent the worker, such as the role within the company.

The introduction of a system-generated mechanism, which exploits the implicit memory effect, can be a valid solution, since the employee do not have to memorise anything and in any case he would not be able to write or confide to anyone the credentials. Furthermore, if the authentication system is based on the gamification principle, it can also be seen as a brief moment of relaxation.

5.2 #2: Secrets Management

Secrets management platforms are software applications designed to support different applications, with the aim to securely storing and accessing secrets to the correct parties and therefore protecting from secret-related vulnerabilities (e.g. secret information in cleartext), both in transit and at rest. In particular, secrets can include several type of items, such as user and system-generated passwords, private certificates, API and other application keys/credentials.

Secrets management tools ensure protection at multiple levels, for example preserving user and application accounts, devices, and other network elements from intrusions, or managing access to cloud accounts and important cloud-based services, or protecting critical systems, storages and databases.

The new methods of deploying applications (e.g. microservices) permit cost-effectively scale services and large systems, arising on the other hand problems concerning securely exchanging secret information. In fact, development teams must share data, configurations and access keys among teams to cooperate on application evolution.

In this context, developers tend to manage secrets through easy, fast and highly unsecure solutions, such as hard-code secrets into the source code, command line entering or shared configuration files.

Secrets Management tools can be secure means for centralization and abolition of secrets sprawl, by encrypting and controlling access to secrets, with fine-grained audit logging.

Actor A developer, who needs to create a new secret for the development of an application.

Objective Successfully access to the required secret in a confidential manner and prevent any illegitimacy.

System The system comprehends the user and the secrets manager program, with the associated trusted technologies (e.g. can include third parties).

Pre-conditions The actor must be registered with valid credentials to the secrets manager program and have the correct authorizations to read or create secrets. Furthermore, Internet access and a browser which imposes a TLS connection are required.

Main success scenario The interaction consists of the following steps:

1. The actor who wants to create a new secret, opens the program and authenticate.
2. The secrets manager program verifies the asserted identity and the assigned policies (i.e. the actor must have permission to create a new secret).
3. The actor creates the secret, which it is securely encrypted by the secrets management tool and visible with the limitations selected by the actor.
4. The secret can be henceforth accessed by other developers or directly from the application, with associated at least reading policies.

Typically, a secret can be accessed based on certain policies, decided by the creator of the secret and associated to authenticated users, who can exclusively operate with secrets they are authorized to. In particular, a so-called “*token*” is generated either manually or not by the creator and associated with the secret, in order to allow other members of the development team or the application (through specific instructions that permit to retrieve the token) to access it, such as in the Fig. 5.2.

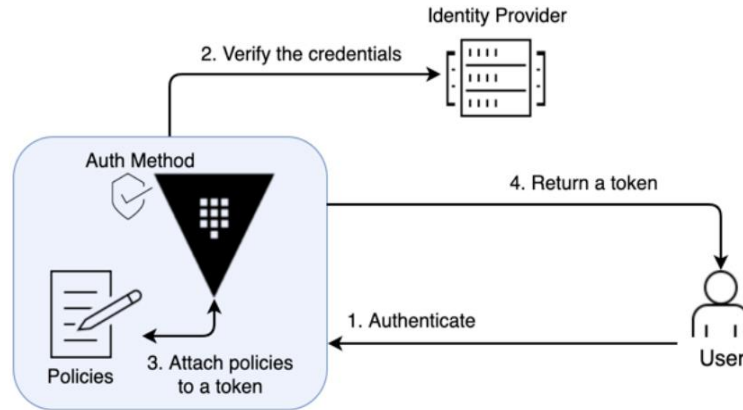


Figure 5.2: Authentication to enter the secret manager from [136]

It is important to notice that tokens and authentication mechanisms can be revoked, in order to preclude access to a specific user.

As a matter of fact, any actual industry standard exists and therefore very specific secret management tools has been implemented by different companies according to their precise needs.

Extensions In first instance, the end-user machine can be infected by a malware, for example a virus or a spyware, and therefore compromise the system security.

The lack of security and proper access management can increase the risk of cyber attacks and theft of certificates or user credentials, such as by Man-in-the-Middle (MITM) attacks and spoofing.

Most of the secrets manager relies on or provide as a choice the user/password authentication method, which is vulnerable to a multitude of previously mentioned issues. This possibility induces the actor to choose this familiar technique over the others, introducing the usual erroneous human factor in generating and managing passwords.

Improvements It is essential to implement proper protection on any system end-user machine, such as aforementioned personal firewalls or malware scanning.

A system-generated authentication mechanism, which is memorable and firmly usable should be implemented instead of the user/password system, to completely evade the human factor from such a powerful tool.

In conclusion, in these systems where the user relies for the storage of their secrets, it is a contradiction to allow to initially authenticate themselves with mechanisms rich in vulnerabilities, such as the familiar username/password. The implementation of a system-generated authentication method, which permits to elude any guessability attack, in combination with the exploitation

of the implicit memory effect, allows the user not to have to memorise additional credentials and prevents them from leaking. In this manner, all the information contained in the secret management platform are securely stored.

5.3 #3: Online payment

Third-party Payment Services Providers (PSPs), such as PayPal, Square or Apple Pay, represent nowadays the most utilised means to easily and quickly transfer money online. As a matter of fact, online businesses have a number online payment methods available, each promising to provide an intuitive and secure checkout experience.

These types of payment services providers process payment information for websites, allowing clients to checkout on different shopping websites, without having to spend further time adding the payment and address information for each purchase.

The card number or bank account information are provided to the payment service at the registration phase and from that moment the client have solely to authenticate in order to authorize the payment.

The case scenario is characterised by:

Actor A client who wants to buy an item from a website.

Objective Successfully complete the purchase and prevent any illegitimacy.

System The system consists of a costumer personal device, the merchant website and a Payment Gateway, which interoperate with the issuing bank to complete the transaction.

Pre-conditions From the user's point of view, the requirements are to possess a device with Internet access and a browser which imposes a TLS connection. Moreover, the client must be registered on the payment gateway's website and a banking account, with valid credentials (e.g. credit card not expired) and have a sum of money in the credit account.

Main success scenario The interaction consists of the following steps, represented in Fig. 5.3:

1. The actor proceeds to the checkout page, after entering the desired items in the cart.
2. The merchant website in general requires the client to authenticate in order to conclude the purchase.
3. The consumer is redirected to payment service's login page, in a secure overlaying window, in order to authenticate and confirm the billing information, in addition to the funding source within the wallet.
4. The merchant receives real-time feedback on the transaction approval from the payment service utilized, once the consumer completes the payment via the payment page.
5. The payment service returns the buyer to the merchant website to review page with the transaction details and the payment status (i.e. success or fail) is immediately communicated both to the client and to the merchant.

Extensions In the system, the PSP assumes the role of the Payment Gateway, which performs the payment interactions essential to the completion of the transaction. On one hand between the buyer and the merchant on the Internet side, and on the other hand between the issuing and the acquiring banks on the private banking network side.

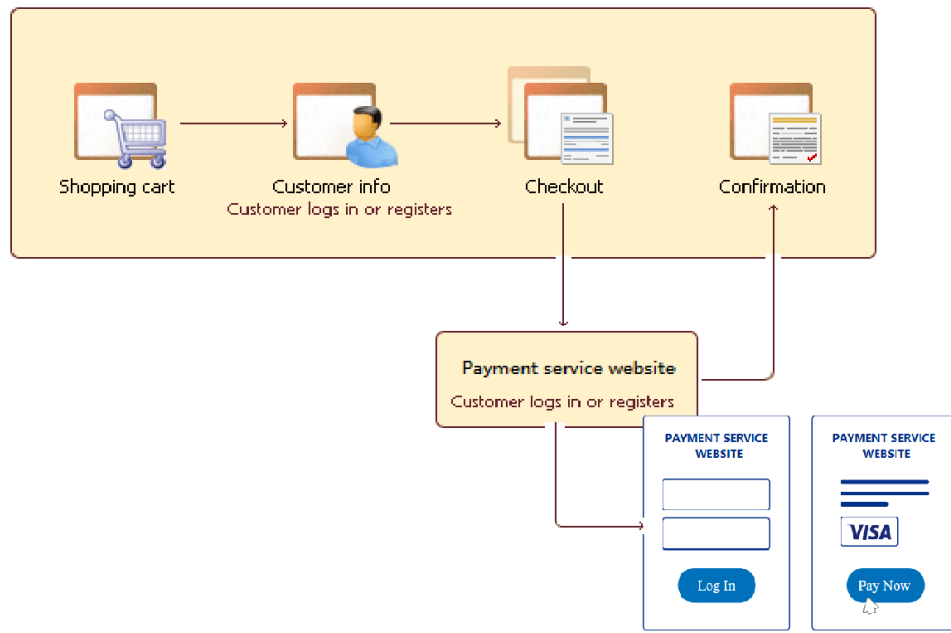


Figure 5.3: Online purchase diagram relying on a payment service

As the entire structure relays on the payment service, the PSPs must offer fraud protection, risk management, transaction reconciliation solutions, reporting and Payment Card Industry Data Security Standard (PCI) compliance as part of their service. Nevertheless, it is the merchant's responsibility to ensure that the payment method offered on the website complies with the guidelines, for example concerning data protection.

As a matter of fact, consumer data protection and privacy are the crucial issues of online payments. However, PSPs typically do not control comprehensively neither the entire supply chain of the payment processing nor the technology and infrastructure security measures involved (e.g. PSPs are responsible for the protection of customers' personal data, not the devices utilized for the purchase).

Therefore, risks concerns the reliability of devices, which store personal information, wireless connections and payment infrastructures, which might lead to major data breach.

Furthermore, fraud and deceptive practices represent crucial issues in online payments, constituting the main security incidents origin. According to the European Central Bank, in 2013, Card-Not-Present payment (i.e. payments via the Internet, post or telephone) achieved the 66% of all fraud losses on the SEPA area¹.

In addition to the traditional attacks performed by hackers to intentionally thief personal data, such as a malware installation or phishing and pharming attacks, identity theft can occur in fraudulent attacks based on profiling and tracking techniques. In practical terms, they are based on the combination of aggregated databases with user personal data, enabling the identification of a person's habits, interests and other personal information.

Finally, DoS and DDoS attacks can target sites or services hosted on web servers and therefore an illegitimate use of information by unauthorized persons or for unauthorized purposes.

Improvements In first instance, it is crucial in order to benefit from all the security measures and to protect the sensitive data stored on devices, to protect devices from malicious software and hacking attacks. In addition the sensitive customer information should stay within a secure

¹ "The SEPA (Single Euro Payments Area) region consists of 36 European countries, including several countries which are not part of the euro area or the European Union." From European Central Bank [141]

payment infrastructure, both in terms of processing and storing data. A limited number of parties should have access to the authentication data, either during or after a payment transaction, in base of need-to-know restrictions.

An effective authentication program should be implemented to ensure appropriate online payment based products and services. In fact, when the buyer is asked to authenticate, the typical technique provided is the username/password mechanisms, which is vulnerable to several widely known attacks and may expose user's information at risk. In this context, considering that two-factor authentication systems are still not implemented neither considered the most usable solution from the user's point of view, a system-generated mechanisms which exploits implicit memory could be a valid alternative. Indeed, the customer would certainly benefit from it, especially in terms of memorization, at the expense of a minimal increase in authentication times.

The PSPs must submit to the guidelines, since robust and comprehensive standards and supporting materials have been developed, in order to improve the security measures regard payment card services. Indeed, the Payment Card Industry Data Security Standards (PCI DSS Standards) comprehends specifications, tools, measurements and support resources for safe handling, process or transmission of cardholder information during the payment operation processing.

Finally, in order to improve the customer acceptance and perceived security of these systems, the disclosure of clear, transparent and complete information should be mandatory. The education of consumers is fundamental in order to detect and avoid potentially fraudulent and deceptive commercial practices.

In conclusion, regarding these payment techniques, it is essential that no leakages of the users credentials occur. Unfortunately, human behaviours jeopardise the security of these mechanisms, which in most cases rely on vulnerable authentication methods. Since these sensitive information gives access to the user's finances, it is essential to prevent them from being revealed or guessed. For this reason, the introduction of a system-generated authentication mechanisms, based on the implicit memory, represent a valid alternative as it does not impose any cognitive effort on the user.

5.4 #4: ATM withdrawal

Automated Teller Machines (ATMs) are computerized systems, which offer to the user a series of activities of a sensitive nature, such as access to cash, confidential information and further several confidential services.

Considering the multiple advantages provided, such as bank workload reduction, contraction of transaction costs and a 24 hours service, they are worldwide adopted.

The case scenario is characterised by:

Actor A client who wants to make an ATM withdrawal.

Objective Successfully complete the withdraw and prevent any illegitimacy.

System The system comprehends the customer, the ATM machine and the bank network to which the ATM is connected.

Pre-conditions The customer must possess a banking account, the activated physical card, valid credentials (e.g. credit card not expired) and a sufficient sum of money in the credit account. The ATM machine must be a secure environment, with severe restrictions regarding physical accessibility to the various components that compose it. The communication with the bank network must be encrypted with a TLS technology.

Main success scenario The interaction consists of the following steps, represented in Fig. 5.4:

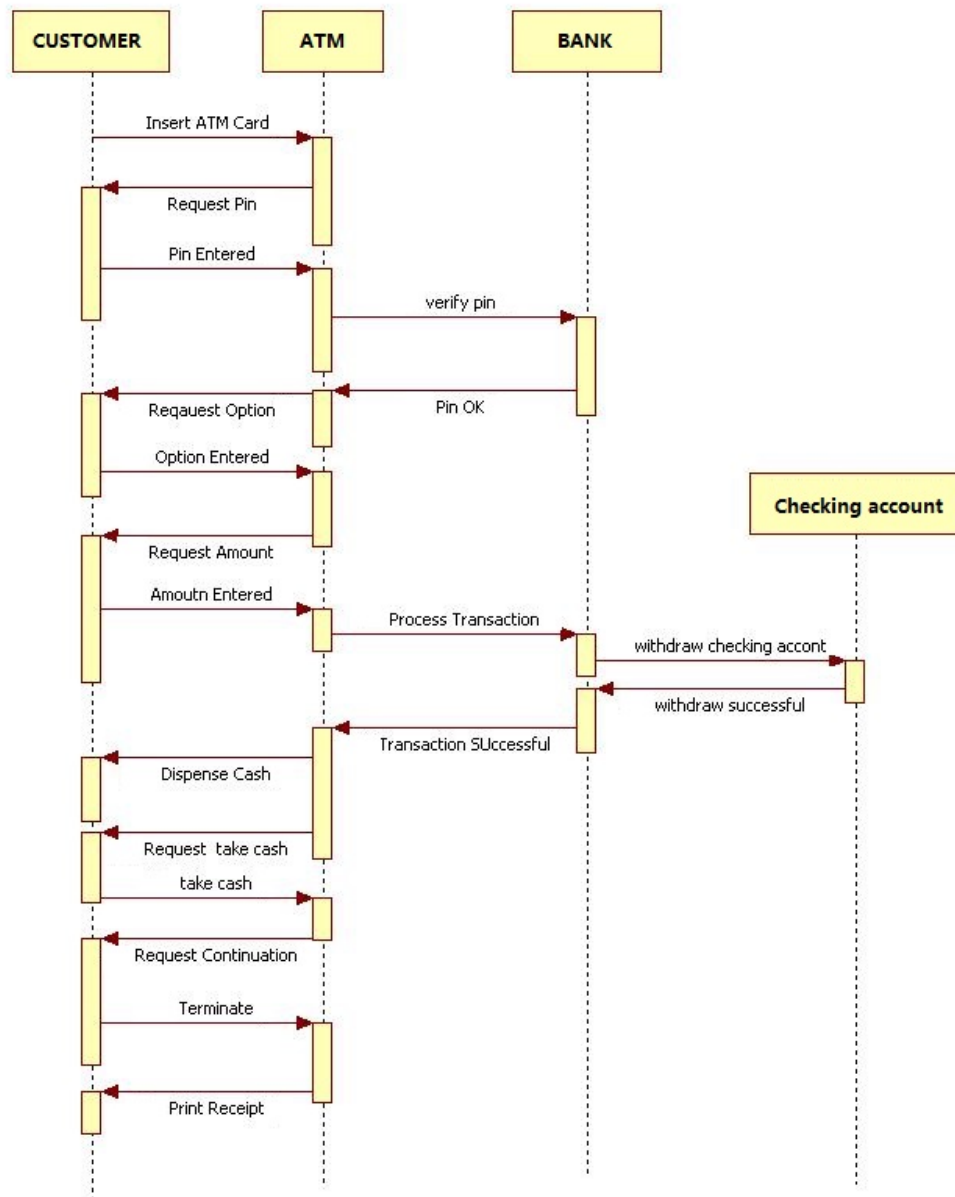


Figure 5.4: ATM withdraw from [137]

1. The actor insert the card into the ATM card reader in order to access the services.
2. The ATM machine acquire the card serial number and requests the authentication secret.
3. The actor authenticate.
4. The ATM machine verifies the information (i.e. card serial number and secret) with the bank in a secure manner. If the credential are valid, the customer is authenticated and redirect to the services menu.
5. The actor select the withdraw option and insert the desired amount of cash to retire.
6. The ATM machine contacts the bank to control the predefined policy limits and process the transaction. The success or failure of the transaction is communicated to the ATM machine, which respectively dispenses the cash or conclude the session.

Extensions Automated teller machines (ATMs) are targets for fraud, robberies and other security breaches, with the aim to obtaining money from the ATM or stealing client's sensitive information.

The connection between the ATM and the bank is either wired or wireless and therefore it can be subject to several attacks. In first instance, network attacks can be performed by an insider (e.g. employee of the bank or Internet provider), who can obtain remotely the access to the network to which the ATM is connected.

An outsider attacker has to tamper the ATM machine in order to access the network, connecting to the modem (or replacing it) a malicious device. In some cases, this operation is facilitated by the location of the modem, which occasionally is positioned outside of the ATM cabinet.

In any case, the attacker is able to attack the available network services (e.g. penetrate a bank's internal network) or attempt man-in-the-middle attacks. For instance, exploiting the vulnerabilities of the network services, such as remote control services, an attacker can disable security mechanisms and controlling output of banknotes from the dispenser.

According to the Positive Technologies report ², in 2018 the 85% of the tested ATM machines was vulnerable to this types of attacks.

Furthermore, it has been demonstrated that it is simple for attackers to perform several different attacks connecting directly to the ATM components. For example, Black Box attacks, which consists of the connection of a single-board computer to the dispenser cable, are notably common. Moreover, the connection of a user-keyboard emulator device to the USB or PS/2 interface of an ATM, allows to exit the kiosk mode³ and command the cash dispenser, easily bypassing the Application Control (intended to prevent execution of unwanted code).

Although major measures has been taken regarding skimming attacks⁴, sensitive data can be stolen during the communications with the processing centre (bank network) or between the ATM operating system and card reader. In the first case, not all the data are encrypted and therefore an attacker who has gained access to the network can sniff sensitive data. In the latter case, the communications are not authenticated or encrypted and therefore the card data are sent in cleartext.

Another technique to steal client information is the set up of a machine that looks like a legitimate, but becomes non-functional after entering the authentication secret. Indeed, any authentication or integrity proof is provided to the user prior to the usage.

Improvements Notwithstanding the technical security risks aforementioned, according to Moncur et. al [138], the introduction to graphical authentication mechanisms can improve both usability and memorability compared to traditional PIN mechanism. In fact, the study proved that a multitude of graphical secrets can be easily remember by the users, with a less pronounced error grade. Concerning the customer security, it is possible to implement a two-factor authentication technique (e.g. additional SMS), with a minor reduction in usability. It is further important to implement a social engineering resistant authentication mechanism, in order to significantly decrease the information theft.

Regarding the security issues, it is necessary to secure the external accessible equipment components and to encrypt any type of communication, in addition to secure and disable unused link-layer and network protocols. Moreover, it is important to strictly reduce user privileges as far as possible and regularly install updates. In addition, authentication mechanisms can be implemented on the devices in order to enforce exclusive access.

²ATM logic attacks: scenarios, 2018 [142].

³"An ordinary ATM user interacts with only one application, which displays information on the screen and processes input from the user. The application runs in kiosk mode, meaning that the user cannot run other programs or access OS functions in any way. ", from ATM logic attacks: scenarios, 2018 [142].

⁴"Installation of unauthorised device to capture data from magnetic stripe of costumer's card. Device will have at least one magnetic stripe read head and will be placed over or within the card entry slot of an ATM or within the card reader itself.", from Terminal Fraud Definitions [143]

In conclusion, although customers are convinced that the PIN mechanism is extremely secure, because it is directly provided by the bank, which in the collective imagination is an emblem of security, the vulnerabilities previously mentioned deny their beliefs. In facts, PINs are frequently forgotten, confused and typically at least mentioned to a trusted person. Furthermore, in general, the physical card is received by the customer in addition to documentation papers, where the PIN is written down, which represents a risk, both in the case if someone steals the sheet or manages to extrapolate the PIN (by photo or photocopy) and in the case of simply loss. For these reasons, the introduction of a system, which do not require cognitive effort for memorisation and it is automatically-generated is a reasonable replacement. Indeed, the user would be required to go to the bank, an institution deemed safe, to register, which could represent the only tedious operation because of the extended times. Afterwards, the client will neither have to remember any secrets in order to withdraw nor be afraid to forget it, as it has been stored in long-term memory, nor be able to tell other people.

5.5 #5: PC unlock

Computer system resources, such as memory, software programs and stored data must be protected. As a matter of fact, unauthorised malicious access to the system can cause severe damage both to the computer and the saved information contained.

Consequently, it is necessary to lock the utilised devices in order to prevent an intrusion and a manipulation either of the machine or the data stored. In addition, the account can be restricted to the local computer, a work-group, the network, or it can be assigned membership to a domain. The two cases are distinguished uniquely from where the user verification occurs.

5.5.1 Local user account

Local users are authenticated by the local system, which store the credential (i.e. username and encrypted authentication secret) on the computer utilized.

The case scenario is characterised by:

Actor A user who wants to access to the personal computer in order to work on a document stored into it.

Objective Successfully complete the unlock of the computer and prevent any illegitimacy.

System The system is composed by the user and the computer, with the necessary resources to complete the action (e.g. local database).

Pre-conditions The local machine has to be a secure environment, specifically it must be not infected by harmful software. Considering that the process to verify the asserted identity runs in the local machine, it is possible to assume that the data are transferred over secure connections.

Main success scenario The interaction consists of the following steps, represented in Fig. 5.5:

1. The actor decides to which account enter and insert the authentication credentials.

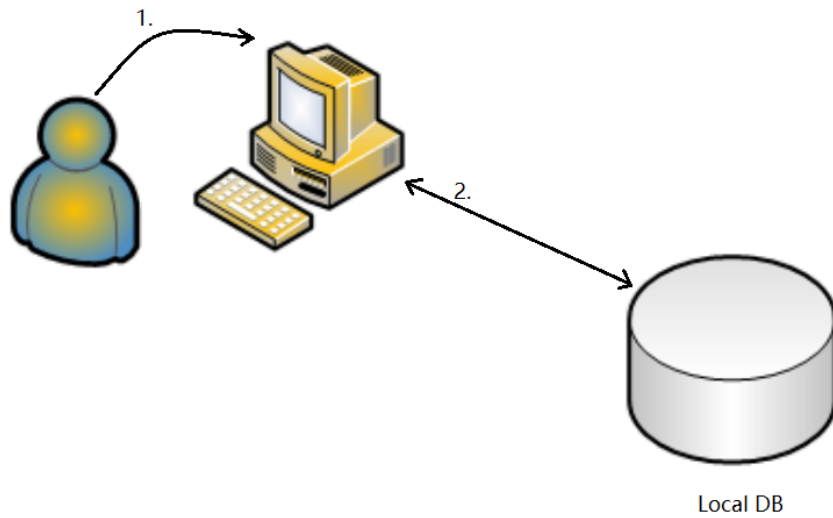


Figure 5.5: Local user authentication

2. The authentication service on the local machine (e.g. Security Account Management, in Windows) verifies the asserted identity, inquiring the ID database located inside the computer (i.e. local memory). The computer examines the list of users and the password file, in order to find a match.
3. The authentication is successfully completed and the actor can access the private account, with the associated permissions and restrictions applied by the system.

Extensions The authentication secret is vulnerable in the case an attacker is able to compromise the system, for example inserting malware into the system or input devices. Computer surveillance permits to monitor the computer activity and indeed the data stored. In addition, compromising the database can invalidate the entire authentication.

Finally, the authentication method implemented must be resistant to the traditional offline attacks, such as brute force attacks and derivatives (chap. 2.2.1).

Improvements It is important that each component of the computer is secure. Indeed, it is recommended to digitally sign and validate the low-level firmware, because otherwise damaging compromises can be performed, arduous to detect and fix.

The authentication method utilised should satisfy the usability and memorability requirements to improve the user's experience. A system-generated authentication system could certainly eliminate the human factor and therefore several vulnerabilities. In addition, a second factor of authentication, such as a token or a biometric parameter, could provide a more secure system, but considering the case of a personal device, it would create an imbalance in the trade-off between security and usability.

Furthermore, in order to avoid unauthorised access, a maximum number of authentication attempts must be declared.

5.5.2 Domain account

In order to overcome the complicated administration of the large number of the computers, peripherals (e.g. printers or network storage), services and users' accounts, the domain concept has been implemented, which include a large population of users on various different computers, registered on a central database located on one or more clusters of central computers, denominated *domain controllers*. These machine are responsible for managing the user authentication and access to the assigned resources within the domain. It is important to observe that computers in a domain can be physical connected on a small LAN or through a WAN.

The case scenario is characterised by:

Actor A user who wants to access to the personal computer in order to print a document.

Objective Successfully complete the unlock of the computer and prevent any illegitimacy.

System The system is composed by the user, the computer and an authentication server, which include a local database with all the domain resources.

Pre-conditions The local machine has to be a secure environment, specifically it must be not infected by harmful software. Considering that the process to verify the asserted identity runs on a server outside the local machine, the transfer of the credentials must be on a TLS connection.

Main success scenario The interaction consists of the following steps, represented in Fig. 5.6:

1. The actor decides to enter the domain account and insert the private authentication credentials.
2. The credentials are sent to the domain controller through the network, with a secure connection.
3. The authentication service on the domain controller queries the ID database, which stores information about members of the domain (i.e. devices and users), to verify the asserted identity. In practical terms, the machine controls the credentials and communicate the access rights.
4. The authentication is successfully completed and the actor can access to the computer network and therefore the shared resources, with the associated permissions and restrictions applied by the local system.

Extensions In addition to the previous possible vulnerabilities, which remain valid in this case, since the credentials are sent to the domain controller through the network, online attacks can occur. In first instance, DoS or DDoS attacks can be performed, preventing the communication and therefore inhibit the authentication. Furthermore, a MITM attack can be executed if the data transfer is not conduct with a secure channel.

Improvements The computer must be not compromise and therefore additional security measures can be installed, such as personal firewalls, malware scanning or file encryption programs. In order to protect the connection the communication must be encrypted and sent through a secure channel.

The user authentication mechanism implemented should be memorable and usable, in particular possibly resistant to social engineering attacks. As a consequence, a system-generated system

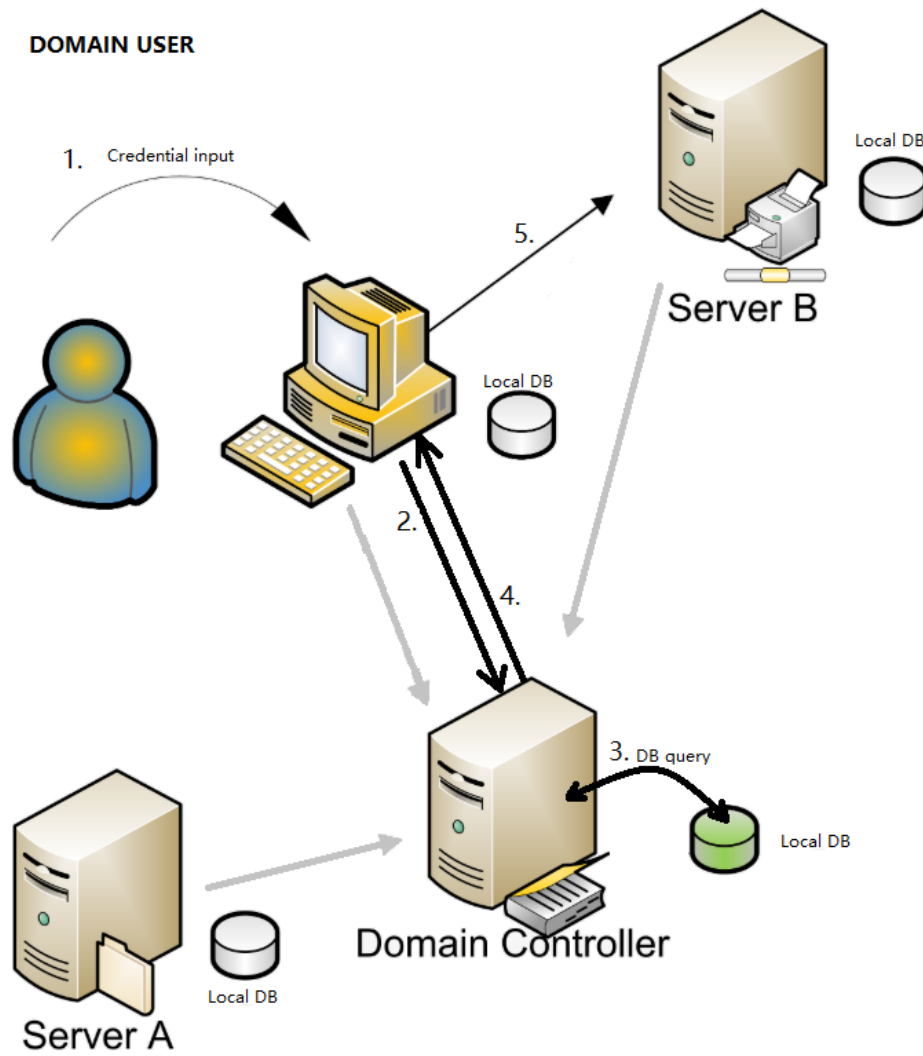


Figure 5.6: Domain user authentication

which relies on implicit memory is a legitimate option, removing the human influence and inappropriate behaviour.

In conclusion, implementing a mechanism which does not require cognitive effort from the user, can lighten the burden of remembering and managing further credentials. Moreover, relying on the principle of gamification, makes it possible to present the power on of the pc as a game to which the user is trained. In fact, although the interaction with computers is nowadays a daily practice, it is not a pleasant action for everyone.

Chapter 6

Usability test

The analysis conducted in the previous chapters led to the development of a prototype, which combines the two powerful concepts of implicit memory and system-generated authentication mechanisms. The aim is to propose an alternative to the traditional user-chosen methods, which can be extremely usable and does not require users to make extensive cognitive effort. For this reason, it has been chosen to implement a system-generated graphical authentication mechanism, which allows a more immediate and simpler memorization.

Furthermore, in order to obtain the most reliable usability evaluation and eliminate any possible introduction of human bias, such as the aforementioned response bias of self-report questionnaire, objective metrics to evaluate user satisfaction have been employed.

In this chapter, the characteristic details of the test are shown.

6.1 Prototype test

The prototype is a system-generated graphical authentication mechanism, based on the concept of implicit memory (see chapter 3), inspired by the work of Joudaki et. al [80].

The aim of the proposed authentication system is to combine the advantages of graphical mechanisms and implicit memory, in order to create an authentication system which requires users a minimal cognitive effort. In this regard, the “gamification” technique (see 3.2.5) has been exploited, as the authentication mechanism is similar to the “hidden object” games, where the user must find a target object within an image.

The main operations provided to complete the usability test are described below (more specific information can be found in the appendix A).

Registration

Registration is the first action required to the user and it is fundamental for the completion of the other tasks.

In order to register, the user must write an email in the specified form of the registration page, which can be a real or a fictitious one, because the system uniquely checks the format of the email. The system permits the user to register through a set of unknown images, randomly taken from a folder proper of the system (not directly stored into a database). In this manner, the user is relieved of the burden of having to select suitable images, which must be disconnected from any possible personal information.

The user is asked to detect the arrow, casually located in the image, recognize its direction

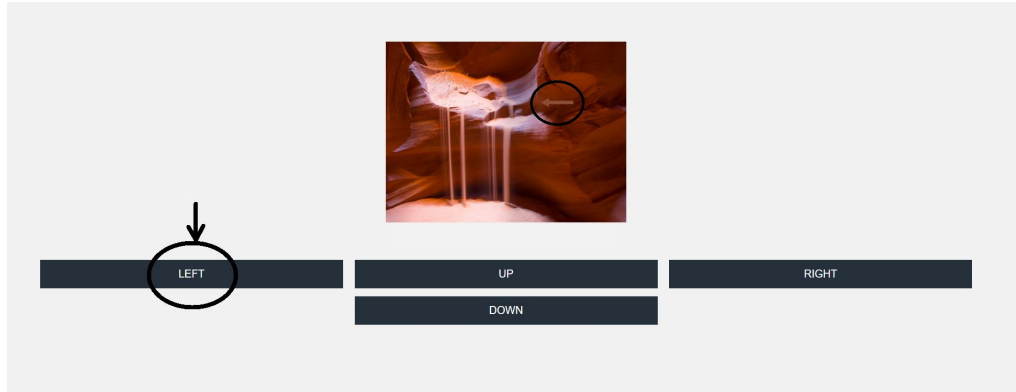


Figure 6.1: Typical page format

and click the respective button (Fig. 6.1). It is important to notice that the arrow is uniquely associated with the image, i.e. neither the direction nor the position ever change.

During the registration phase, no time limits are inserted as the user has to become familiar with the mechanism.

It is important to notice that the user must not memorise any information, neither the images nor the directions nor the sequence of images (images are indeed presented in a casual order).

In this phase, in case of error there will be no consequence for the user.

Training

The user in this phase is trained to identify, within each system-selected image of the associated set, the direction of the target symbol (i.e. an arrow), which indeed represent the actual secret. This phase is essential in order to trigger the implicit memory effect, by means of repetition of the same actions.

The training is composed by the random repetition of the entire set of images for a total of 4 rounds¹. The training phase is mandatory in order to correctly register.

A time limit is set during the training session, within which the user must identify the target and click the correct button. The objective is to allow the user to acquire the sufficient visual-motor skills to pass the subsequent login phase, where it is essential to rapidly recognise the location of the target in the image (i.e. visual skill) and click the correspondent button (i.e. motor skill). Furthermore, in this manner it results more difficult for an attacker to memorise the user's sequence.

The secret is composed by the directions of the targets and it is securely conserved into a database.

During the registration process, which include the training phase, a series of relevant data can be collected for the future analysis. In particular, timing data are of paramount importance, because allow to deduce the user's initial approach to the system. In fact, the time that elapses between the loading of the image and the click on the button, can be utilised as a mental effort information (i.e. the difficulty to find the target). Moreover, the mouse clicks and patterns and

¹According to [80] "the cueing effect arises after the fourth block of 16 displays."

the requests for help can be acquired and considered as an index of the users' comprehension of the mechanism. In addition, an error rate can be extrapolated from incorrect entries and exploited to presume the complexity of the system.

Login

The login process represents the verification of the acquisition of the secret, which allows the user to access their personal page and execute secondary operations.

In contrast to the registration phase, the login phase consists of a single round, in which the images of the training phase are presented to the user in addition to supplementary random images, never seen by the user. In this manner, the system is protected from an attacker, who tries to memorise the secret exclusively looking at the login images, since not all of them are associated with the user.

A time limit is inserted, within which the user must identify the target and click the correct button. As a consequence, each incorrect entry or no entry can be considered errors and used as secret knowledge discriminator. In fact, a trained user is supposed to be able to locate the target and click the correspondent button in few seconds (according to the work of Joudaki et. al [80] 3 seconds are sufficient).

The task is deemed successfully completed if the user inserts a sufficient number of correct entries.

In the same manner as registration, both errors and mouse clicks and patterns can be recorded and considered as an index of complexity and users' mental effort for the further analysis.

Secondary operations

In order to obtain a more realistic and comprehensive analysis, additional tasks are requested to the participants. They refer to subordinate operations, such as the username change, which can exclusively be performed after successfully authenticating. As a result, capturing additional information by the completion of a series of different auxiliary tasks, a more peculiar user attitude can be delineated.

Analogously to the previous cases, information are collected regarding successful completion, timing and number of mouse clicks and patterns, help requests and errors.

Logout

The logout represents a necessary operation, which permits to return to the initial page from the personal page of the user.

In particular, after the completion of both the registration and login phases, the user is asked to click on the correspondent button and complete a final questionnaire, in which general questions about the entire experience are proposed.

This operation indicates the end of the entire experiment.

6.2 Usability evaluation structure

As previously mentioned in Chapter 4, the usability evaluation will be based on the analysis of the three main usability characteristics, respectively effectiveness, efficiency and satisfaction. The main purpose is to adopt uniquely objective metrics, in order to provide a neutral study, independent from subjective influences.

In total, 22 participants are involved, selected in order to guarantee heterogeneity both in terms of age, gender and experience in interacting with systems of this type.

The age range varies from 17 to 60 years old participants, with different frequencies of use and capacities with authentication systems and generally with IT systems. In particular, half of the population for the test works, while the other half is composed by students from different faculties, both scientific and humanistic.

Effectiveness and efficiency The entire set of data collected during the entire execution of the test (e.g. errors, completion and time information) are further exploited to evaluate the system's effectiveness and efficiency.

In particular, the numbers of errors in entering a wrong direction and failures in the registration, training and login phases will be counted, in order to provide an indication of the complexity of the system. Furthermore, the time data are analysed in order to obtain the time intervals need to each user to complete a task. In particular, registration and login times are considered fundamental to comprehend effectiveness and efficiency of the prototype.

It is important to mention that the entire set of operations executed by the user are monitored by a detailed log, where all the information previously cited are stored.

Satisfaction In respect to satisfaction of the users, two different strategies are adopted:

- **Objective metrics**

In order to obtain an unbiased evaluation of the system, the physiological reaction of the participants are registered.

Whether possible, eye-tracking and ECG capturing programs are employed to estimate users' reaction to the system. The first one is an eye-tracking technology, which identifies the gaze movements of the individual by means of the webcam of the participant. As a result, it can be recorded and extract the mental effort necessary for different tasks.

The second technology records the Heart Rate Variation (HRV) by means of a specific bracelet, in order to capture eventually significant changes of the heartbeat of the individual. Consequently, through a cardiogram application which create indicative graphs, information about the perception of the prototype can be evinced.

Furthermore, during the execution of the test, mouse clicks and patterns are collected through a web analytics site and utilised as additional objective metrics for the analysis. In fact, continuous and precise mouse movements can be indicators of a positive attitude, while segmental and scattered movements can suggest a more negative impression.

- **Subjective questionnaires**

In order to obtain a comprehensive understanding of the satisfaction of the users, additional final questionnaires are proposed to the participants. In this manner, it is possible to compare the results of the object measurements, dictated by the physiological behaviour of the person, and the subjective opinion of the individual. Indeed, objective metrics do not discern between the positivity or negativity of the recorded emotional state.

After the completion of each presented task, a series of specific questions are proposed to the participant, in order to acquire more information about the sensations felt and permitting a more detailed analysis of the data afterwards. In addition, a final self-report survey on the subject perceived experience of the interaction with the system (e.g. concerning emotional state, attitude and effort) is provided. The questionnaire are composed of several questions, regarding different aspects of the prototype, such as the security perceived or the familiarity with the mechanism utilised.

6.3 Implementation

In this section the implementation choices are specified, in accordance to the guidelines defined in the previous section.

6.3.1 Prototype

In first instance, the number of images to be associated with the user has been set to 10, in order to improve the usability of the system (Joudaki et al. [80] utilised 16 images). In addition, the number of session in the training phase is the minimum required by the human brain to properly memorise the location of the target in the image, i.e. 4.

The time limit imposed in the training and in the login phases is set to 5 seconds, considering the minor set of images and training sessions.

6.3.2 Usability evaluation

Effectiveness and efficiency

The entire set of data regarding effectiveness and efficiency is collected by the log file. The log file of each participant is analysed through an Excel spreadsheet, which allows a rapid and simple manipulation of data.

The times of registration, login and of the first and last training phases were considered the most important, in order to examine the feasibility of the system. The latter allow to observe that the implicit memory effect has actually occurred, as from the first to the last training phases there must be an improvement in timing.

Moreover, the number of errors in entering the right direction of the arrow and failures both in login and registration are gathered, in addition to the number of help requests.

Satisfaction

Regarding the satisfaction characteristic of usability, the information are collected through the support of the technologies described below:

- Objective metrics

The eye-tracking data are collected with *OGAMA (Open Gaze And Mouse Analyzer)*², an open source software which analyses eye and mouse movements in slide-shows, by means of the webcam of the participant's computer. Since the program does not permit to collect data online, a different auxiliary test has been proposed to a sub-portion of the participant population. This brief test recreates the registration and the login processes, through a presentation, which maintains the same structure of the pages presented in the prototype (e.g. the time limit of 5 seconds). In this manner, the eye-tracking heat-map calculated can be compared with the heat-map and pattern-map represented by the movements of the mouse.

The second technology employed in the objective usability evaluation regards the acquisition of the Heart Rate Variation (HRV), through a bracelet with an optical heart rate monitor. In particular, the Apple Watch series 3 has been utilised, specifically the Nike+ edition and the ordinary series 3, which rely on the same technologies³. The mechanism permits to observe the heart rate every 5 seconds, after the first capture of the beat, which is carried out for one minute, in a state of rest (i.e. arm horizontally resting on a desk). The display shown is represented in Fig. 6.2. This also remains in line with the timing imposed for the expiry of the images, which permits to capture the heart rate even for each image displayed. Additional online mechanisms have been implemented in the code in order to obtain an

²For more information see <http://www.ogama.net/>

³For detailed information regarding the mechanism of data collection see the section “*In che modo Apple Watch misura la frequenza cardiaca*” in <https://support.apple.com/it-it/HT204666>



Figure 6.2: Typical Apple Watch screen for Heart Rate capture

optimal analysis of the data. For instance, the *Inspectlet* site⁴ has been employed in order to monitor the participant attitude on the site test. It registers the sessions of the users, with the video recording of the mouse clicks and patterns. In addition, it generates different types of heat-maps based on the mouse movements, which are compared with the eye-tracking heat-maps obtained through the OGAMA program.

- Subjective questionnaires

All the questionnaires implemented in the test are created with Google Form and to facilitate users in understanding the questions, they have been written in Italian. Three different questionnaires have been inserted in three different phases of the test, specifically after the registration phase (which includes the training process), after the login and at the end of the entire test.

The registration and login questionnaires are structured in the same manner. They are called “*HOW DO YOU FEEL?*” and interrogate the user regarding the actual emotional state immediately after the completion of the task. They are composed by three questions, which are:

1. How did you feel during this phase?
2. Does the time spent approach your initial expectations?
3. How easy was it to spot the arrow?

The final questionnaire is composed by 21 questions, which are:

1. Have you ever heard of other authentication methods besides passwords?
2. If so, what other methods do you know?
3. In your personal experience, do you think that a new authentication mechanism is needed besides that of alphanumeric passwords?
4. What was your first reaction to the system?
5. How would you evaluate the potential of this new authentication mechanism?
6. How innovative do you think this authentication mechanism is?
7. Would you use this authentication mechanism in everyday life?
8. Would you replace your typical authentication mechanisms with this new mechanism?

⁴For more information see <https://www.inspectlet.com/>

9. How safe do you think this mechanism is?
10. How easy was it to understand the steps to take?
11. Is the registration time what you expected?
12. Is the login time what you expected?
13. What do you think of the timing of this authentication mechanism?
14. How easy was it to spot the arrow inside the images?
15. Do you think the size of the images is adequate?
16. How distracted were you from the background images?
17. In order to locate the arrow, how much better do you consider abstract images than those representing a real scene?
18. Would you change your opinion about the system, if for security and memorability reasons the number of images increased?
19. Do you have vision problems?
20. If yes, do you think this mechanism may not be suitable for people with your same problem?
21. During the whole experience you felt (multiple options are: enthusiast, curious, agitated, frustrated, quiet, confused, other).

The data collected from the responses have been directly analysed by Google and the results permits the confrontation with the objective data acquired by mean of the aforementioned objective metrics.

Chapter 7

Results Analysis

In this chapter the results obtained from the usability evaluation are presented, following the order of the tasks performed by the participants. In order to provide a more immediate understanding, the data are always expressed as a percentage and accompanied by explanatory graphs. Moreover, additional observation regarding the emotional state during the different phases contribute to a comprehensive analysis of the information collected.

7.1 Context

The test has been executed whenever possible under the physical supervision of the examiner, otherwise through a Skype call with the participant, in order to observe and listen to any user reaction (it was not explicitly requested to think aloud).

The environment conditions marginally affected the execution of the test, even in the case of remote testing, as the participant was required to perform the test in a room, which conforms to the ambient of the examiner room. In particular, it was requested not to perform the test in an outdoor or highly illuminated with natural light location, because it would strongly affected the results and the impression of the whole system.

7.2 Registration

In the registration phase, the choice to not insert time limits has allowed to obtain very fluctuating results regarding timing. In any case, the participants remain under 4 minutes (the maximum time collected is 4.09 minutes), with an average registration time of 1 minute and 55 seconds (Fig. 7.1).

In fact, the participants, who had been warned in advance of the absence of time limits, allowed themselves to relax in order to locate the arrow and develop a method to find it. A feedback is noted in the recording of the beats, which in this first phase is generally characterised by a decrease of up to 5 bpm when the arrow is not easy to find.

Furthermore, the mouse pattern recordings in most cases represent slow and continuous movements over the image displayed, which may reflect the calm and concentration of the participant (Fig. 7.2).

The data obtained do not reveal any anomalies which could penalise the prototype with respect to long times, as 2 minutes on average can be considered an acceptable time for registration. During the registration phase, only 2 participants (9.1%) committed a single error, which was detected and corrected in the successive training phase.

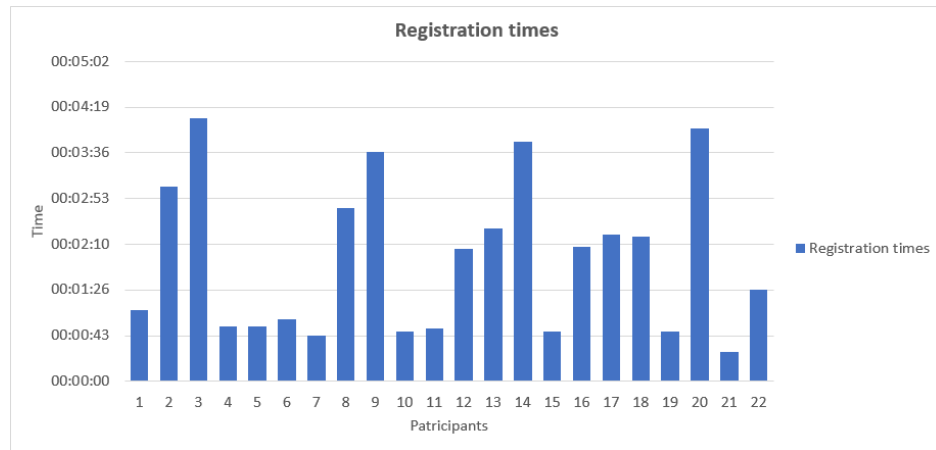


Figure 7.1: Registration times of each participant.

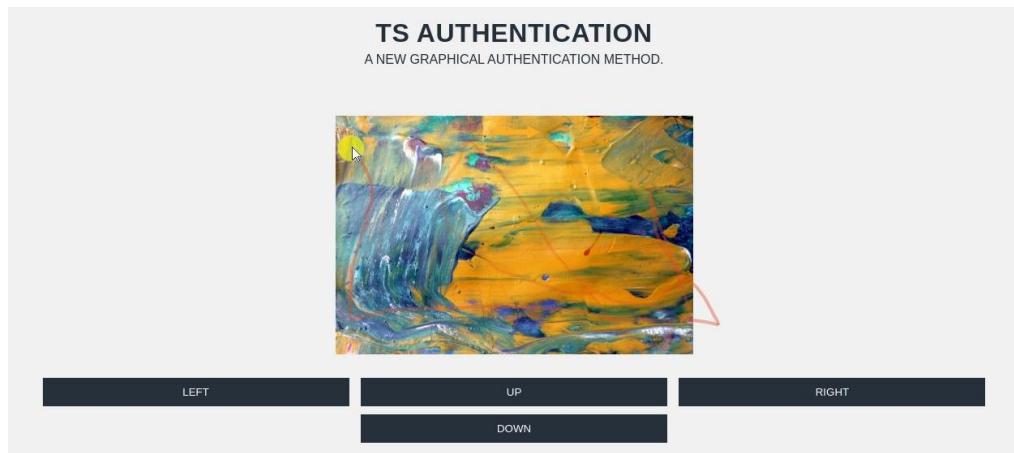


Figure 7.2: Example of the mouse pattern recording of the preferred method to find the arrow in the image.

7.3 Training

During this phase it is possible to observe the effect of the implicit memory, both in the different timings (Fig. 7.3) and in the number of errors (Fig. 7.4) of the first and the last training sessions.

Regarding times, the average time calculated for the first session is 32 seconds, while in the last session is 25 seconds.

In a single case the timing of the last training session exceeds the first.

Considering that no errors was made by the participant in question, neither in the registration phase nor in the training sessions, the heart rate variability is considered. It is possible to notice that in the initial training sessions the heartbeat is increased (6 bpm more respect the end of the registration) and the time between two successive images is a maximum of 2 seconds, indicating

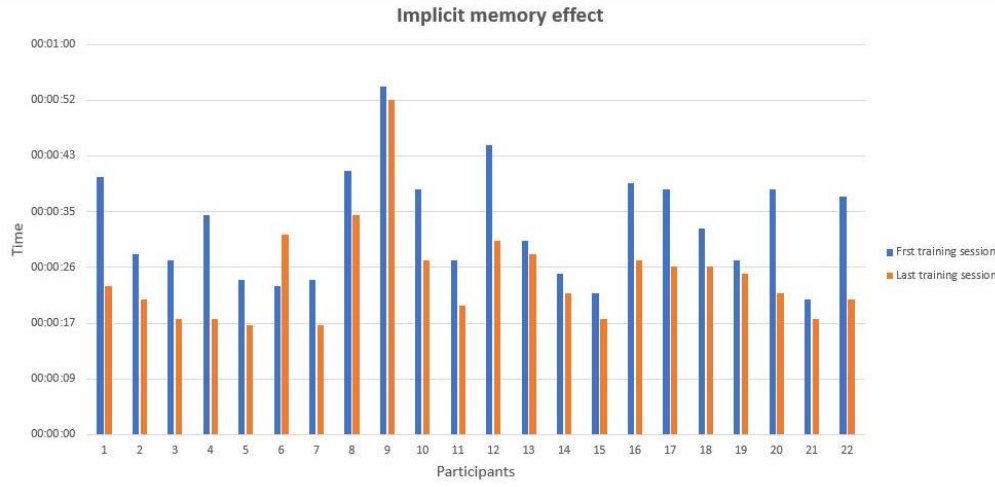


Figure 7.3: Times of the first and the last sessions.

concentration. In the last session the heartbeat decreased of 5 bpm and the time between two successive images reaches 4 seconds per image. It is possible that the participant felt bored by the duration of the training phase and slowed the pace.

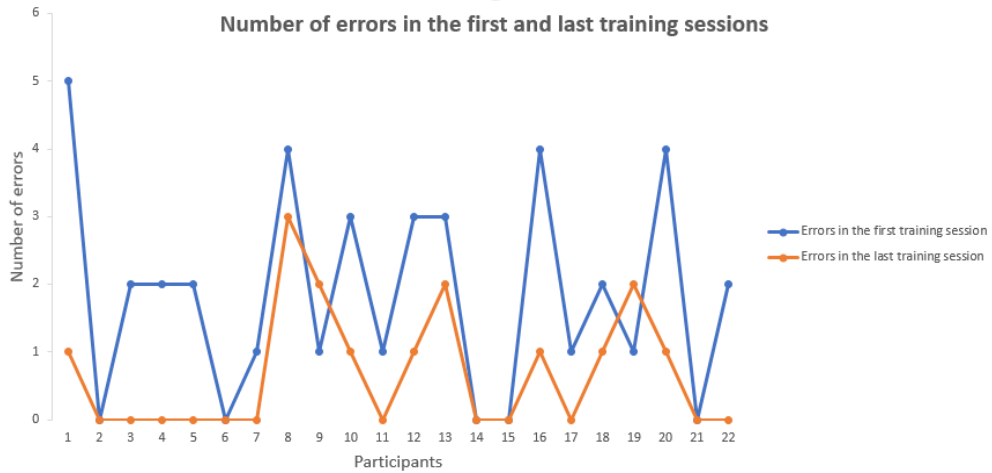


Figure 7.4: Errors of the first and the last sessions.

Regarding the errors, the maximum number collected is 5 errors in the first session and 3 errors in the last session.

The majority of the participant decreased or eliminated errors between the two phases. Only two exceptions have been noted, in which the errors in the first training phase are greater than the second. The reason can be found in the heart rate captured during the test: in the first case, the participant reduced the beats, suggesting a general relaxation, which led him to be more confident (as he felt to comment during the execution of the penultimate phase of training) and therefore decrease the threshold of attention. In fact, until the fourth session he had made only one error. On the opposite side, in the second case, it has been registered a crescendo of beats during the

training process, due to an excitement in knowing how to find the arrows, which has resulted in a state of agitation at the moment when it has not found them any more.

In general, in this phase it is observed the major increase of the heart rate, probably caused by the inclusion of a time limit. Although it was specified that there would be no consequence in the case of error, an average of 5 to 10 bpm variation has been reported for each participant. However, in the questionnaire presented immediately after this phase, to the question concerning the emotional state the 52,2% of the participants answered “calm”. It is an interesting result, considering the heart beat variation in some cases reached 15 bpm more compared to the registration and the mouse pattern recordings display a fast and discontinuous movements, uniquely in the section of the directional buttons. These observations suggest an altered emotional state of the user, who could either be enthusiastic or frustrated, which were two options of the response, but not calm.

This result could be a consequence of a rationalisation of the entire registration phase, which include different emotional mutations and the participant is obliged to choose one.

A final comment concerns the overall registration times (i.e. registration and training times), which on average require 3.52 minutes and therefore can be considered acceptable. In fact, in the registration questionnaire, uniquely 3 participants (13.6%) gave a negative evaluation of the timing.

7.4 Login

The login phase obtained the most positive results. In first instance, only 4 participants (18.2%) failed the login, 3 of which (i.e. 13.6 % of the total) need only one retry.

The successful logins are within a highly acceptable time range, between 18 and 41 seconds (Fig. 7.5). The only exception is given by a user who waited for the maximum insertion time,

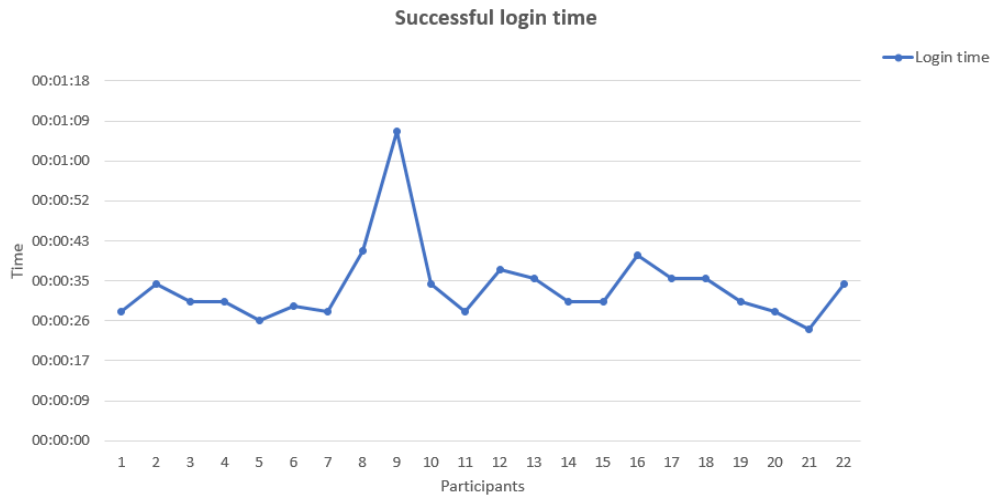


Figure 7.5: Timing of the successful login.

before clicking on the correct button. The motivation was spontaneously given by the participant, who wanted to challenge himself. In fact, it maintained a constant high heart rate during the entire login process, which indicates concentration and agitation.

Regarding the login timing, 18 participants (81.8%) have been positively surprised about the rapidity of the process.

Nevertheless, it is interesting to notice that 6 of the 11 who voted 4 out of 5 in the question “Does the time taken approach your initial expectations?”, specified aloud that in practice exceed their expectations. It was intriguing observe that, in these cases, the heart rate of the participant increased about 2 or 3 bpm,during the decision process.

Additional interesting results concern the ease of locating the arrow, to be compared with the registration responses. In fact, in the questionnaire immediately after the login process, 9 of the participants (40.9%) answered “easy to find” (voted 4 out of 5) and 5 participants (22.7%) “very easy to find” (voted 5 out of 5), in contrast to the registration phase, where respectively 8 (36.4%) ad 1 (4.5%) participants provide the same answers. Analogously, a difference emerges regarding the emotional state during the two phases. In fact, in the registration phase, in addition to the inaccurate response selecting the “calm” option, one half of the remaining participants (47.8%) indicated a negative emotional state of frustration or confusion. Whereas in the login phase, the users responded more properly, according to their aloud thoughts and heart rates, revealing an increased positive attitude towards the mechanism. In fact, the 52% answered “calm”, but in this phase no discrepancies has been found with the heart rate variability, which was higher but more constant.

Furthermore, the remaining participants (48%) decided to write the real emotions through the “other” option, which can be grouped in a general exiting state. In addition, a greater precision

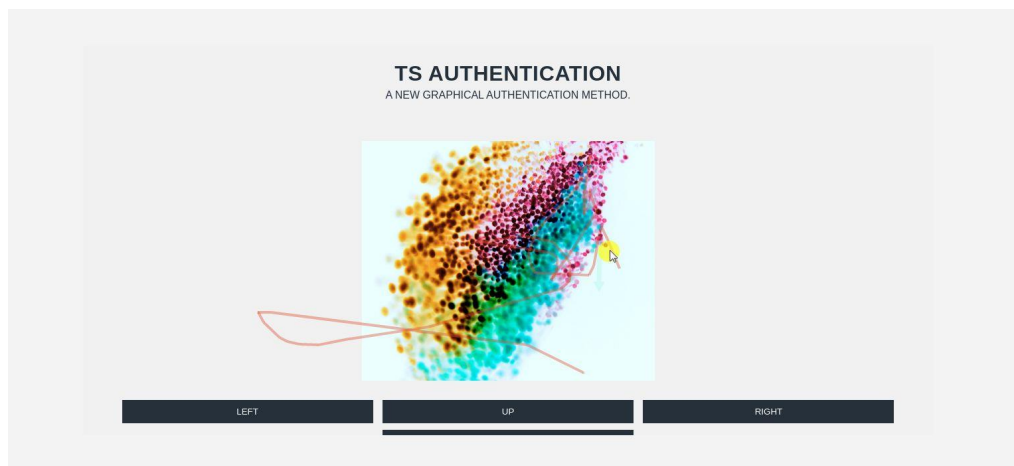


Figure 7.6: Example of mouse pattern of the registration phase

in the actions to be performed can be found in the mouse patterns during the login phase. In fact, compared to the patterns of the registration (Fig. 7.6) or training phase (Fig. 7.7), the mouse is directly pointed to the button to be clicked (Fig. 7.8).

In the same manner, the heat-maps obtained by the clicks tracking, demonstrate a vivid performance improvement in the login phase (Fig. 7.9) in respect of the registration (Fig. 7.10), as the clicks are concentrated only on the directional buttons.

Interesting results are derived by comparing the different eye-tracking technologies adopted.

The results suggest a rapid and undemanding memorisation, which exalted users, who want to genuinely retry the login as they specified it is equivalent to an entertaining game. Some of the participants (27.3%), indeed, described aloud the pleasure to hypothetically authenticate with this mechanism, as a sort of an enjoyable break from work.

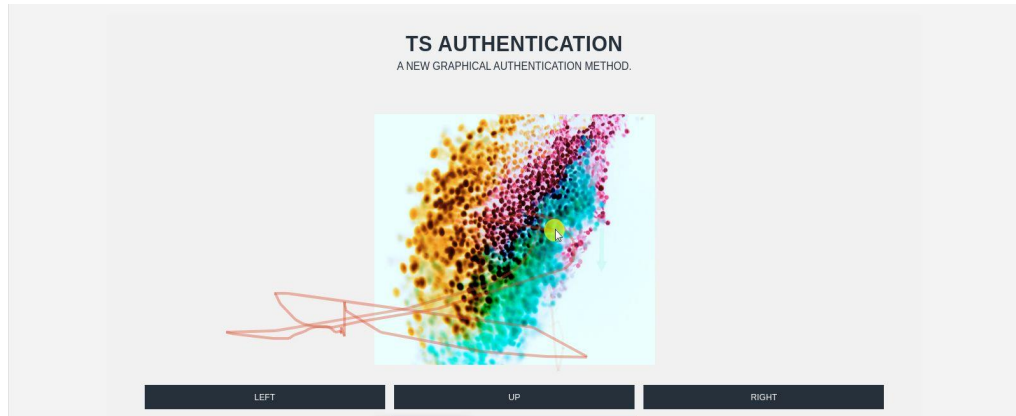


Figure 7.7: Example of mouse pattern of the training phase

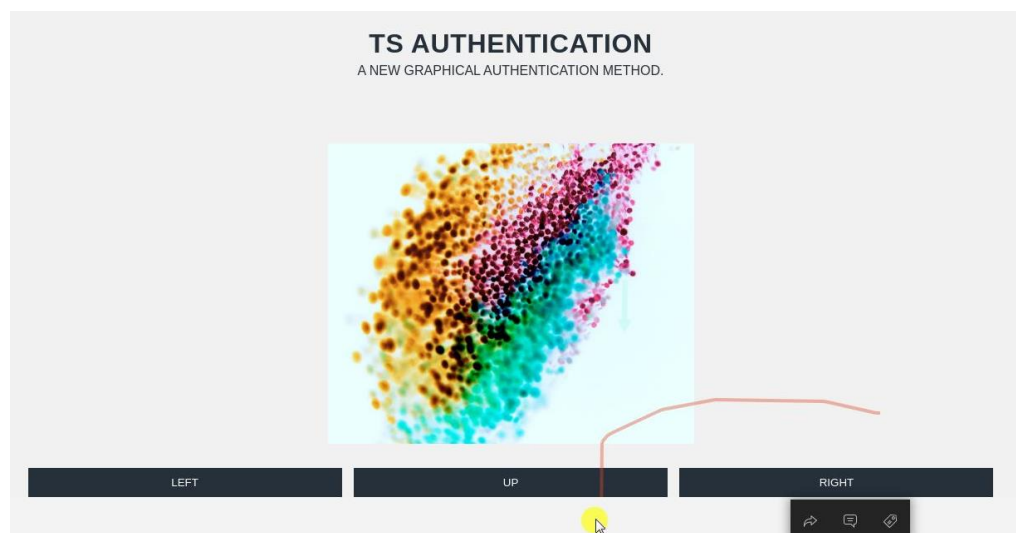


Figure 7.8: Example of mouse pattern of the login phase

7.5 Final questionnaire

The final questionnaire was utilised in order to collect the sensations of the participants about the prototype and the whole experience.

A series of general questions is proposed to comprehend the level of consciousness of the participants regarding user authentication methods and further evaluate the results obtained concerning the prototype.

Each participant, except one, claimed to know multiple alternatives to passwords (Fig. 7.11) and voted in favour of introducing a new authentication method, dissimilar to passwords, because either is strongly convinced of it or had difficulties with passwords (Fig. 7.12).

No one of the participants disagree with the possibility of replacement, only 3 (13.6%) selected the “I do not know” option, as a consequence of their inexperience with IT systems in general.

As a measure of the satisfaction of the proposed mechanism, the answers to the questions

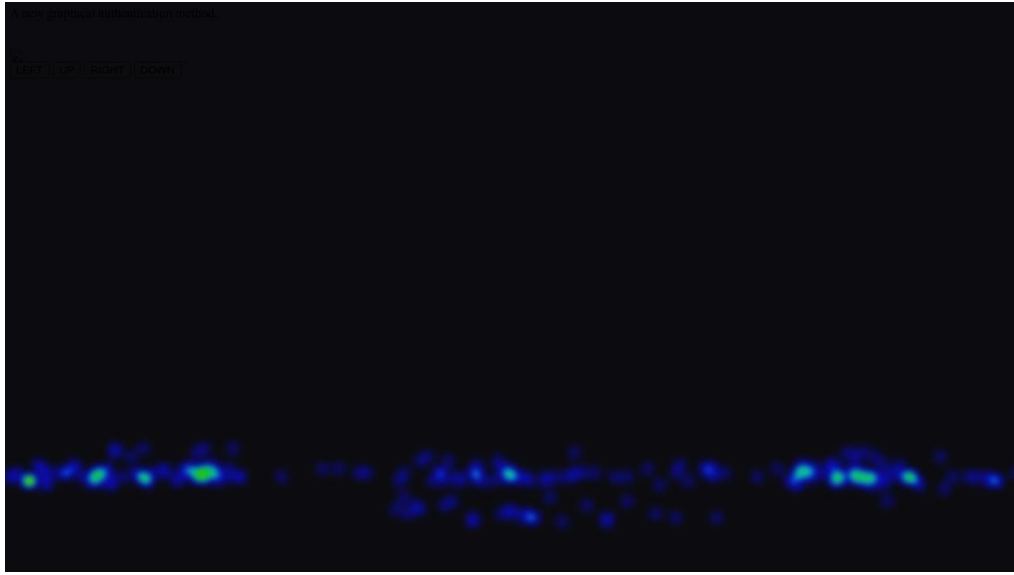


Figure 7.9: Example of mouse clicks of the login phase

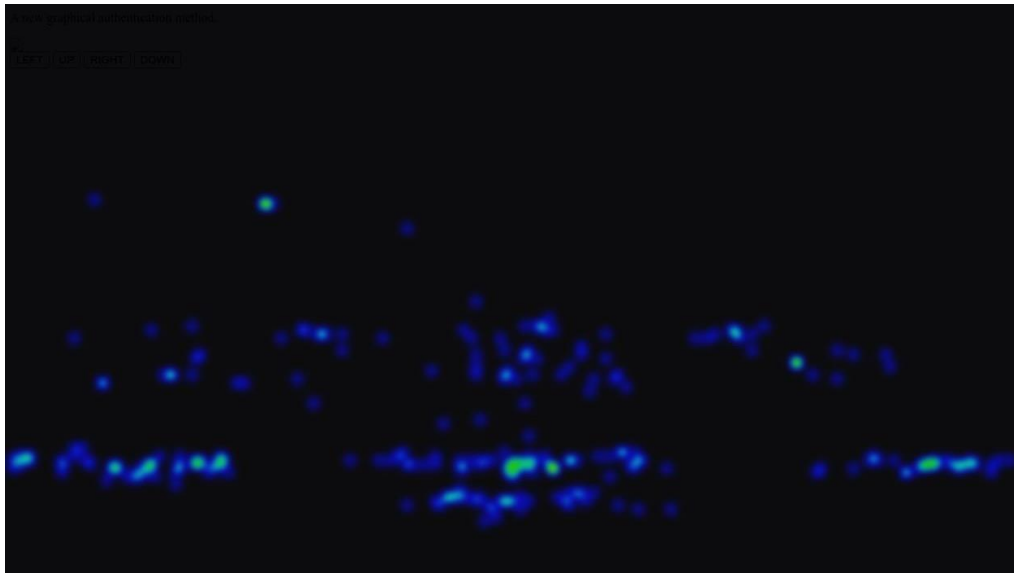


Figure 7.10: Example of mouse clicks of the registration phase

regarding the possible employment of the prototype in everyday life and as a substitute to the current methods, are fairly positive. Indeed, the majority of participants (54.5%) expressed preference of implementation for selected areas, such as work environment, the 31.8% for all occasions and the 13.6% in no circumstances (Fig. 7.13).

Nevertheless, the majority (54.5%) admit that would not replace it with methods considered safer in their opinion, for example the token for the banks.

An additional fascinating result is represented by the final responses concerning registration and login timings. Indeed, it is evident the influence of later processing of the entire experience, as a marked diversity in the diagrams can be observed, respectively in Fig. 7.14 and Fig. 7.15.

Regarding the image format, no noteworthy results emerged. The participants stated that the image size was adequate and the difference between abstract or real-scene background images

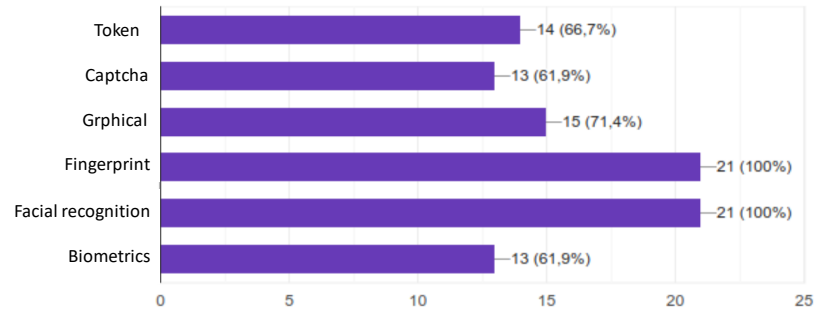


Figure 7.11: Alternative authentication methods known by the participants

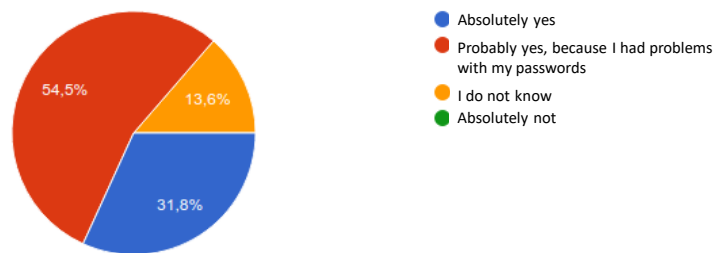


Figure 7.12: Different authentication method necessity responses

did not influence their goal to locate the arrow. Nevertheless, heterogeneous answers were given regarding the general distraction of the background image, as shown in Fig. 7.16.

Interesting heart rate data have been captured in this conclusive phase. As a matter of fact, it results simple to discover the uncertainty of the user by an increase in heart beats. Indeed, when the participant had to make a decision, a cognitive effort was evident in the choice of the answer. In the moment of the choice, the heart beat returned to normal and stabilised for all the questions to which the answer was sure.

It was fascinating observing this decision-making process, both through the variability of the heartbeat and physically noting different attitudes, because it revealed and confirmed the difficulty of self-report questionnaires to be objective in providing the user's opinion. Indeed, a great portion of the participants (86.4%), before giving an answer on which was undecided, tried to involve the examiner in the reasoning, in order to seek approval. Furthermore, most

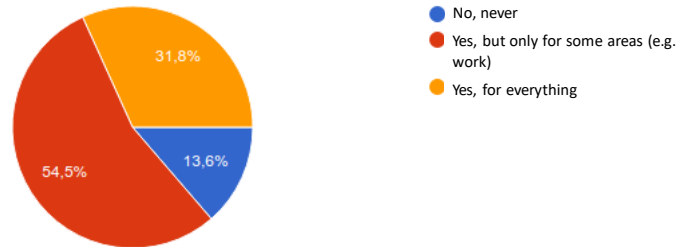


Figure 7.13: Everyday life implementation responses

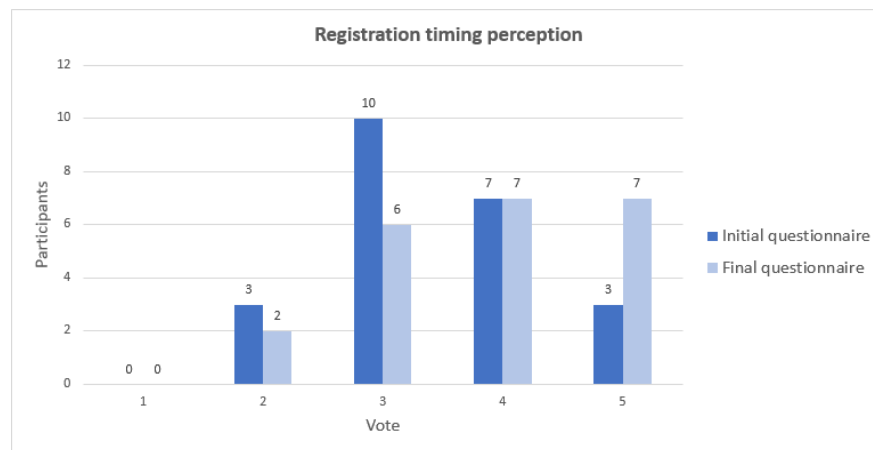


Figure 7.14: Registration timing responses compared

of the times, the hesitation resulted in a medium response, towards neither of the two extremes, positive or negative.

In conclusion, the final emotional perceptions after the entire test execution are presented in Fig. 7.17. The diagram refers to a multiple choice question, in which the totality of the participants selected more than one state.

It is possible to notice that the two predominantly chosen options are “calm” and “curious”. The first one, although the previously mentioned considerations, refers to the emotion experienced by the user during the login and the conclusion of the test. In fact, according to the heart rate recordings, except for sporadic peaks in indecision instants during the final questionnaire, all the participants stabilized the beats on their resting value, indicating a general relaxation. The “curios” option selection can be justified by the final reprocessing of the whole experience, when

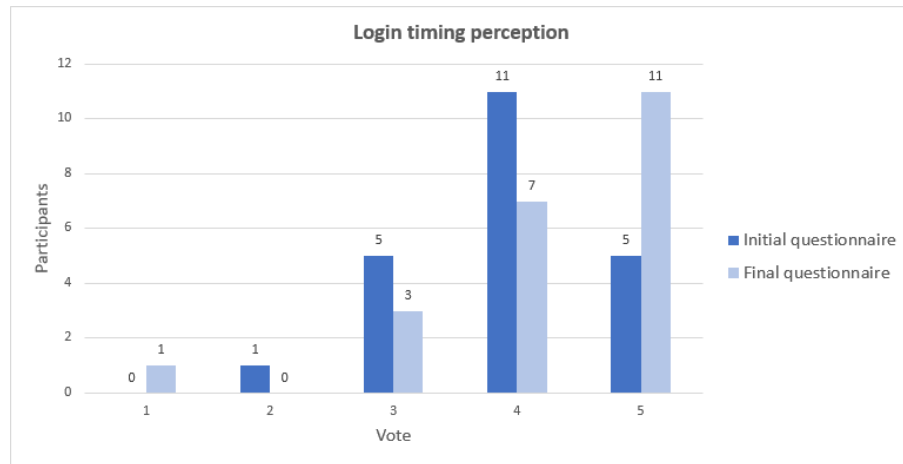


Figure 7.15: Login timing responses compared

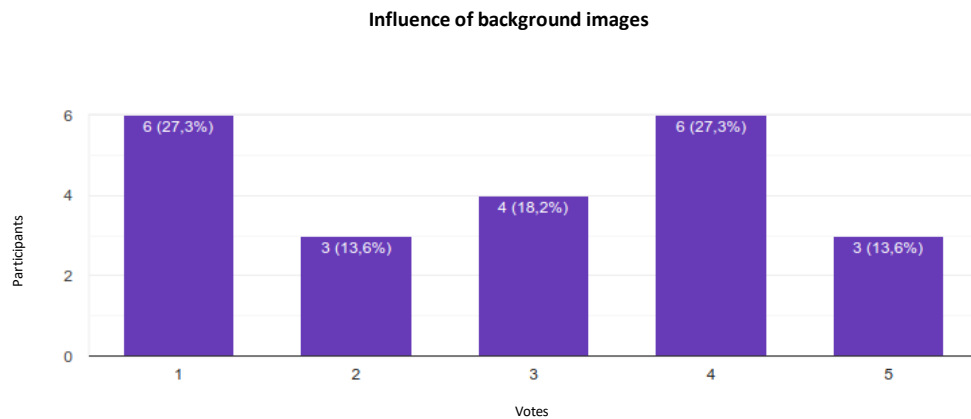


Figure 7.16: Background images influence responses

the user has become truly aware of the performance.

7.6 OGAMA test

A sub-portion (i.e. 5 individuals) of the participants was subjected to a further test, aimed at collecting eye-tracking data.

Since the mechanism employed does not allow user interaction during the recording of the eye movements, participants were forced to look away as soon as the arrow was found. In this manner, the results are not compromised, because the user does not spend superfluous additional time on the image.

In order to obtain the most reliable data, each user had to repeat the entire authentication

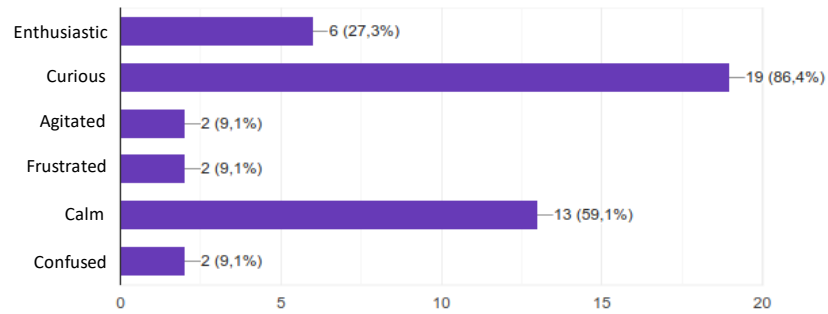


Figure 7.17: Final emotional state responses

process, with images never seen in the previous test. As a consequence, the participant cannot be influenced by the unconscious knowledge of the image.

Therefore, the outcomes do not significantly differ from those of the mouse-tracking, in terms of timings and heart rate variability. In fact, although a minor improvement in both areas, derived from the fact that the system had already been approached in the first test, the cognitive effort registered is comparable.

In particular, during the registration phase, the participants behaved similarly to the previous assessment, employing their own personal technique to find the arrows in the images. It is interesting to notice that 3 of the users (60%) preferred to utilise the mouse in order to explore the image. As a consequence, the information about the eye-tracking and the mouse-tracking are particularly correspondent. Analogously, the rest of the participants, who minutely analysed the image uniquely through the eyes, obtained corresponding results.

In the training phase, a more evident difference can be perceived. In fact, although both results of eye-tracking (Fig. 7.18) and mouse-tracking (Fig. 7.7) suggest an altered state of the subject under examination, through the first mechanism it is emphasised by the large number of short and confused eye movements.

It is also interesting to note in the figure (Fig. 7.18) the implicit memory effect, as the gaze is concentrated uniquely in the area surrounding the arrow.

During the login phase, the performance of the participants have improved in the same manner of the first test. Nevertheless, user behaviour is remarkably more unequivocal through the utilisation of the eye-tracking mechanism. Indeed, the pictures derived from the eye movements indicates that, in the login phase, two fixations in average are sufficient to locate the arrow. Two different examples are shown below in Fig. 7.19 and Fig. 7.20. It is important to notice that the areas marked in these two last images result shifted from the actual point of interest. The distortion, which remains in the surroundings of the arrow, can be caused by the adoption of a not excellent webcam.

In conclusion, although the final outcomes of the tests can be considered equivalent, the employment of an eye-tracking mechanism allows to provide more precise information regarding user attitude towards the system. In fact, the mouse can act uniquely as an indicator of the user movements, but eyes represent a more reliable source in order to evaluate the attention and cognitive effort of a person.



Figure 7.18: Eye-tracking example of the training phase

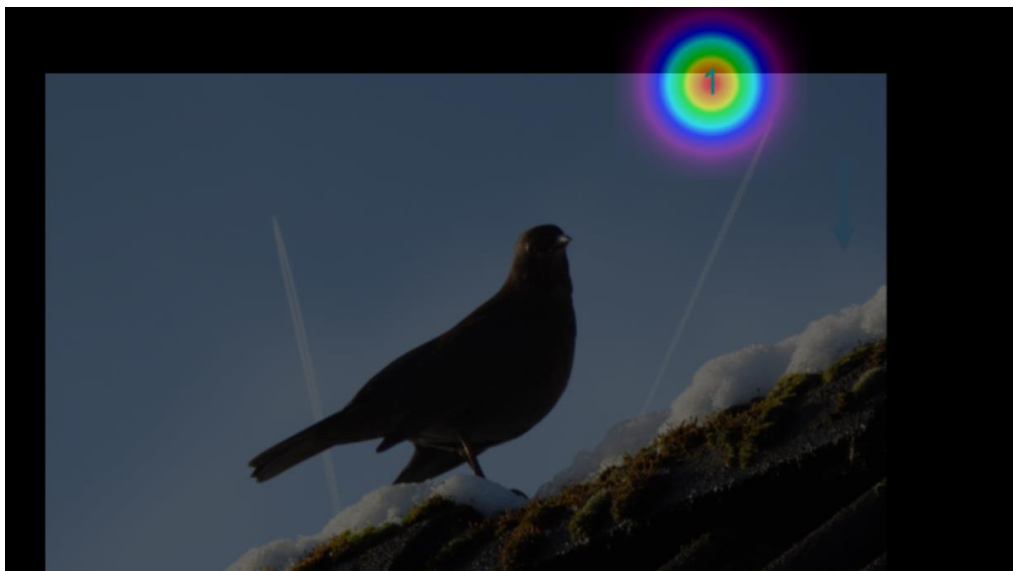


Figure 7.19: Eye-tracking fixations: the best case



Figure 7.20: Eye-tracking fixations: the worst case

Chapter 8

Conclusion and future work

According to the analysis of the state of the art conducted in the first part of the thesis, the necessity to develop innovative authentication methods that equally balance security and usability is evident.

The predominance of security over usability resulted in a poor acceptability of new the techniques or in counterproductive human behaviours, which undermine the security of the systems.

Considering that humans represents the weakest link in the security chain, it is fundamental to move towards an ever greater absence of the erroneous human component, deepening and subsequently exploiting the different potentials of the human brain. In fact, considering the continuous integration of IT systems into everyday life of people (e.g. IoT), it is necessary to develop mechanisms that exploit human skills to improve interaction with these systems.

In this regard, the aim of this thesis was to present an alternative to the traditional user-chosen authentication methods, which can be extremely usable and does not require users to make extensive cognitive effort. For this reason, system-generated authentication mechanisms were analysed and in particular, techniques which exploit implicit memory, i.e. an ability of the brain to unconsciously acquire and maintain information, have been examined.

Based on the aforementioned investigations, a prototype was developed in order to study the usability of these novel mechanisms. It has been chosen to implement a system-generated graphical authentication mechanism, which allows a more immediate and simpler memorization. In the usability evaluation, objective metrics were adopted to verify the authentic perception of the users, especially concerning user satisfaction.

The results obtained from the tests conducted on a total of 22 users of different age, gender and IT experience, are positive and certainly promising.

Indeed, 90.9% of the test participants expressed interest in this new authentication technique, affirming the need to overcome the traditional username/password method.

From the users' point of view, the only flaw in the system are the registration times, which induced the participants to express their interest to implement the prototype in certain areas, such as the working environment.

In my personal opinion, the potential of this system is sincerely high and it needs to be explored.

Excellent results were also obtained from objective metrics, which reveal adequate timing, in accordance with the graphical nature of the system, good performance and minimal cognitive effort.

Since the results have been considerably optimistic, it is necessary to present a series of improvements to further enhance the prototype:

- In first instance, in order to facilitate users, it could be appropriate to insert the possibility of operating with the arrow keys on the keyboard. In fact, it could be more practical and even decrease the registration and especially login times. Furthermore, it could a secure

solution as a possible attacker may not follow the mouse movements, which can be extremely explanatory, and learn the sequence.

- From the perspective of a possible real development of the prototype, it is essential to enforce the security of the system. In fact, it is important to take into consideration that the research has focused on the usability, not its security.

First of all the data saved in the database must be protected with an advanced encryption method and not only by the database password.

It may be interesting to observe if the insertion of distractors in the images (preferably, in my opinion, blended as the arrow) could improve security, for example regarding shoulder surfing attacks, and consequently also the perception of security of the entire system by users. For the same reasons, it is possible to moderately increase the number of images, both in the registration and the login, proportionally adapting the error threshold. In this case, I personally consider it necessary to maintain the minimum number of training sessions, in order to preserve the usability of the system, which could otherwise become tedious for users.

- The prototype could be further enforced by the implementation of a second factor of authentication, such as an eye-tracking or a keystroke dynamic mechanism. These techniques could be used to implement a continuous authentication mechanism. In this context, it could be fascinating examine the exploitation of ECG techniques, through bracelets or other means accessible to a large part of the population, considering that the heart rate varies substantially from person to person, as it has been noted during the experiment performed.

I would like to conclude with a quote from Grace Hopper, a pioneer of computer programming and a personal influencing female figure:

“Humans are allergic to change. They love to say, ‘We’ve always done it this way.’
[..].”

These concise words can incisively summarise the motivations of this thesis and represent a basis for reflection concerning the direction to be taken in authentication systems.

The necessity for change is evident and it is of primary importance to introduce new mechanisms, which lead to a fair balance between usability and safety.

In the end, although humans are reluctant to change, their finest characteristic is the spirit of adaptation, which would guide them in the migration towards new authentication methods.

Appendix A

User manual

A.1 The system

The prototype you are going to test has the aim to provide a new method of authentication, where the user must not make any cognitive effort.

It is based on the concept of *implicit memory*, which represent the ability of the human brain to learn information without focusing on the actual memorization of them.

In fact, you do not have to create any password nor make any kind of decision. The password is uniquely associated with the user by the system and it must not be memorized. The password is composed by a set of images, not directly stored into a database.

The user is request solely to detect an arrow in the image, recognise its direction and then click the respective button, located under the image.

A.2 Test execution

The user is first redirected to the homepage, where is required to sign in.

In order to start the registration, the user must click on the “SIGN IN” button in the menu on the left.

The user is now redirected to the registration page, where is asked to insert the email to be registered. This email can be invented or a real one.

Then the user is asked to click the “START” button in order to begin the registration process. After the registration process is completed, which include the training session, the user is redirected first to a quick questionnaire and then to the personal page.

In the personal page the user can change the username, book a trip on a bus and delete it, logout or delete the account. It is preferable in this first phase not to delete the account, because it would mean registering again.

The user who logouts is redirected to the homepage and is requested to perform the login. Analogously to the registration, after the login the user is redirected first to a quick questionnaire and then to the personal page, where the above mentioned secondary operations are permitted.

After the login phase, and performing some or all the secondary operations, the user can decide to either logout or delete the account.

No limit has been imposed on the number of times a user can repeat tasks during the test session.

After each task the participant is redirected to a brief questionnaire, regarding the emotional state, attitude and effort experienced during the completion of the activity. At the end of the test, the user is asked to complete a final questionnaire (by clicking the “FINAL QUESTIONNAIRE” button in the Homepage), in which general questions about the entire experience are proposed.

Below a more detailed specification of each page is presented.

A.3 Homepage

The homepage is the principal page, where the user is redirected at the beginning of the test and anytime an error occurs.

On the left, the menu is shown, with the buttons that respectively allow login or registration. On the upper right corner there is a help button, represented only by a “?” character (Fig. A.1). This button permits the user to open a different window with the user manual, in order to consult

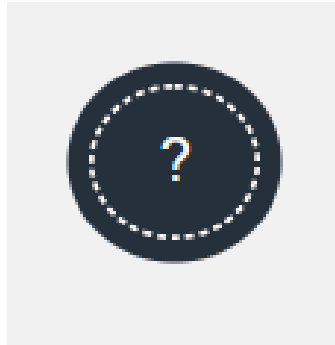


Figure A.1: Help button

it. The help button is present in each principal page (e.g. sign in and login pages).

A.4 Registration

Registration is the first action required to the user and it is fundamental for the completion of the other tasks.

The first action required to the user is to insert the email. It can be a real or a fictitious one, the system will not verify the real existence of the inserted email.

Consequently the user is redirect to another page, where is informed that the registration process is about to start.

After clicking the “START!” button, the user will be redirected to the real registration page. In this page will appear an image and below 4 buttons, which indicate the four possible directions of the arrow associated with the displayed image.

The user is asked to detect the arrow casually located in the image, recognize its direction and click the respective button (Fig. A.2).

The registration phase is composed by the random repetition of the set of images, which will represent the password associated with the user.

It is important to notice that the user must not memorize any information, neither the images nor the directions nor the sequence of images (images are indeed presented in a casual order).

In this phase, in case of error there will be no consequence.

A.5 Training

After the first stage of registration, the user must be trained with the personal associated images. The objective of the training phase is to allow the user to acquire the sufficient visual-motor skills

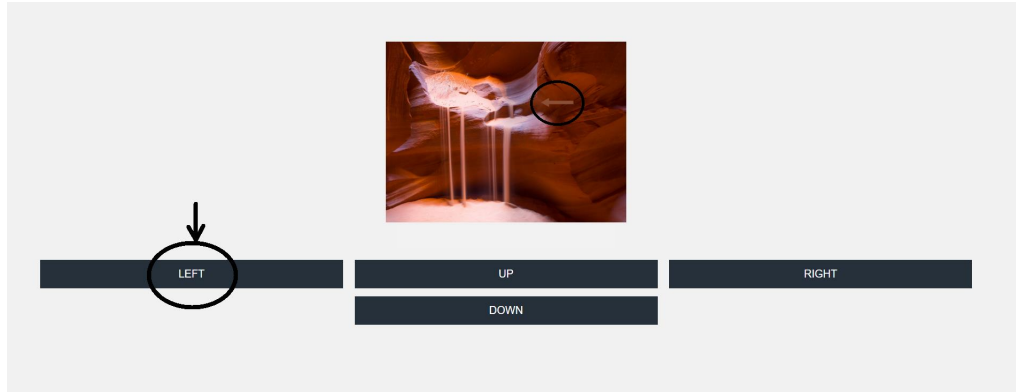


Figure A.2: Typical page format

to pass the subsequent login phase, where it is essential to rapidly recognise the location of the target in the image (i.e. visual skill) and click the correspondent button (i.e. motor skill). In order to achieve these abilities, the images associated with the user are randomly displayed for several times. In addition, to improve the skills, a time limit is imposed, within which the user must complete the actions.

The page that is presented is graphically identical to the registration page and the operations to be performed remain the same: the user must detect the arrow and click on the corresponding button.

In this phase, in case of error there will be no consequence.

After the completion of the training phase, the user is redirected to the personal page.

A.6 Login

The login process represents the verification of the acquisition of the secret, which allows the user to access their personal page and execute secondary operations.

In contrast to the registration phase, the login phase consists of a single round, in which the set of images of the registration phase are presented to the user in addition to supplementary random images, never seen by the user.

A time limit is inserted, within which the user must identify the arrow and click the correct button. Each incorrect entry or no entry are considered errors and used as secret knowledge discriminators.

The user in order to correctly authenticate must make a maximum of 3 errors, otherwise the login fails.

At the end of the login process the user is redirected to the personal page.

A.7 Personal page and secondary operations

In order to obtain a more realistic and comprehensive analysis, additional tasks are requested to the participants. They refer to subordinate operations, such as the username change, which can

exclusively be performed after successfully authenticating (i.e. sign in or login).

In the personal page the user finds a series of buttons, each of which represents a secondary action to be performed and finally the button to log out. It is important to be noticed that, after the registration, it is preferable for the user to log out instead of deleting the account. The reason is simple: once the account has been deleted, the user must register again, executing all the steps.

At the bottom of the personal page, the current route of the minibus is represented, with the various routes booked by other users. Since there are 4 seats available on the minibus, before booking a trip it is advisable to check in advance if the number of passengers exceeds the maximum for the route the user wants to book.

A.7.1 Book your trip on the minibus

This operation permits the user to book a maximum of 4 seats on this imaginary bus, accurately called Minibus. The user can select from a drop down menu the route to be covered.

After clicking on the “Book your trip” button”, the user is redirected to the booking page, where the number of passengers must be insert and the points of departure and arrival selected. To complete the reservation click on the “Conclude” button.

If the booking is successfully completed, in the personal page, the departure and arrival points are coloured in green. The reservation will not be completed in the case of insertion of invalid itineraries or excess of the maximum number of people.

In order to book a different trip, the user must delete the previous one.

A.7.2 Delete your trip

This button permits the user to eliminate the trip previously booked, without entering any information. By clicking the button the trip is automatically deleted.

After deleting the reservation, the user is able to make a new one.

A.7.3 Change username

This action permits to modify the username from the email to a preferred name. It is important to notice that to authenticate the email is mandatory: you cannot login with your new username. In fact, after the logout the username will not be stored and it will not appear in the personal page unless the user changes it.

A.7.4 Delete account

The user who wants to delete the registration to the system can click on the correspondent button and agree to eliminate the account.

After this operation, in order to re-utilise the authentication system the user must register again.

A.8 Logout

The logout represents the ultimate operation, when the user finishes to perform the desired operations.

Once logged out, the user can login.

A.9 Installation manual

In order to proceed with the test, the technical environment must first be prepared. The folders needed are provided in a .zip file, named “*TSAuth_Test*”. It is suggested to export the “*TSAuth_general*” folder on the Desktop, in order to facilitate future operations.

A.9.1 Web server

The mechanism to be tested needs to have web server support installed on the computer utilized for the test.

If the user already has one, the “*TSAuth_general*” folder can be directly inserted where required by the application utilized.

If the user did not have to download XAMPP, proceed to the database configuration section. Otherwise the most updated version of XAMPP can be downloaded at the following link:

<https://www.apachefriends.org/it/index.html>

In this case, once the installation is complete, the steps to be followed in order to prepare the web server to correctly work are specified below:

- Open the control panel (double click to open the program);
- Click on the “*Start*” both at the Apache line and at the MySQL line;
- The “*TSAuth_general*” folder must be placed inside the folder “*htdocs*”:
 - Go to the XAMPP Control Panel;
 - Click on the “*Explorer*” button on the right side of the panel;
 - A folder will be opened;
 - Search for the “*htdocs*” folder and enter it (double click);
 - Copy the “*TSAuth_general*” folder in this folder.

Proceed to the configuration of the database.

A.9.2 Database

In case the user didn’t have to download XAMPP:

- Search within “*TSAuth_general*” the file named “*conf.php*”;
- Change the values that allow the access the own database;
- Create a new database named “*tsauth*”;
- Import the “*tsauth.sql*”: the file contains the initial configuration of the database for the testing. DO NOT MODIFY this file.

In case the user had to download XAMPP:

- From the XAMPP Control Panel, at the MySQL line, click the “*ADMIN*” button;
- The user is redirected to the phpMyAdmin site (also reachable at <http://localhost/phpmyadmin/index.php>);
- Different databases are displayed on the left, click on “*New*”;
- Name it “*tsauth*” (all lowercase!) and then click the button “*create*” on the right (Fig. A.3);
- The user is redirected to the database newly created, which has to be initialised:
 - At the top of the page, click on the section “*Import*” (Fig. A.5);
 - Click on “*Scegli file*”;
 - Search for the “*TSAuth_general*” folder in the system (e.g. in the folder exported at the beginning from the .zip file);
 - Open the “*tsauth.sql*”;

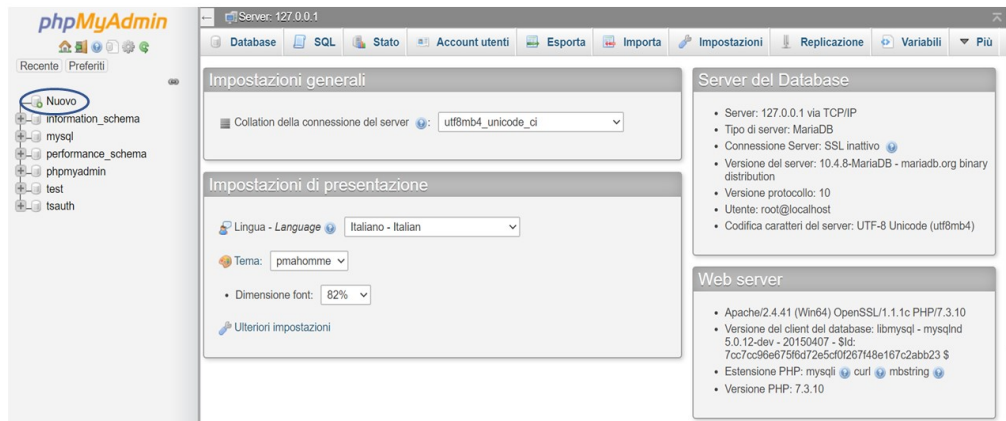


Figure A.3: Creation of the new database

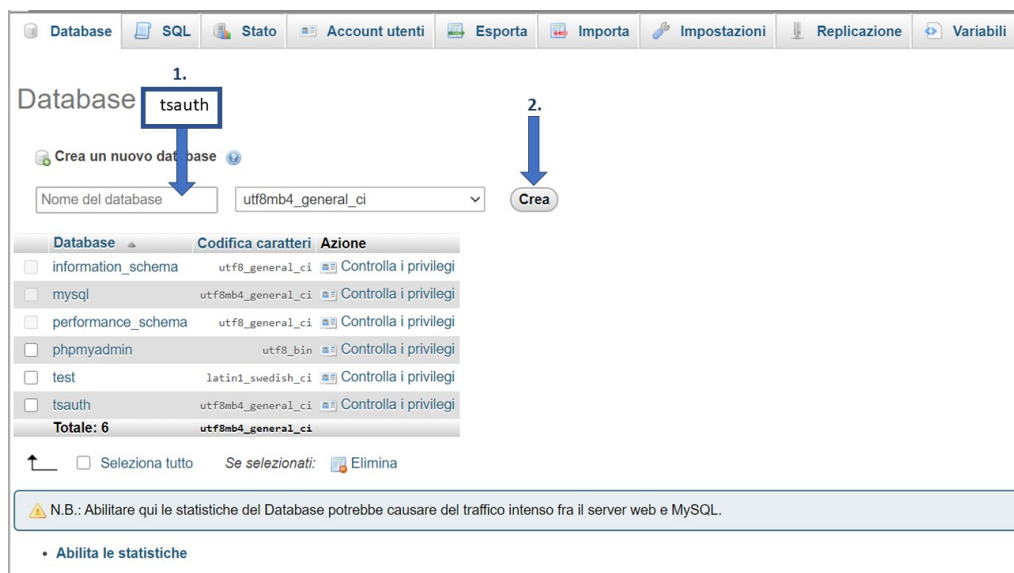


Figure A.4: Creation of the new database: set the name

- Scroll down and click the button “Esequi” (Fig. A.6);

In order to improve the security of the database, it is preferable to insert a password:

- Return to the main page, by clicking on “phpMyAdmin” in the upper left corner (or at the url <http://localhost/phpmyadmin/index.php>);
- Click on “Account utenti” in the top bar (Fig. A.7);
- Click on “Modifica privilegi” (Fig. A.8);
- Click on the button at the top “Cambia password” (Fig. A.9 (1.));
- Insert a password of your choice in the specific area (Fig. A.9 (2.));
- Click on the button “Esequi” at the bottom right;

Now, in order to be able to successively access your database, the phpMyAdmin configuration file must be updated:

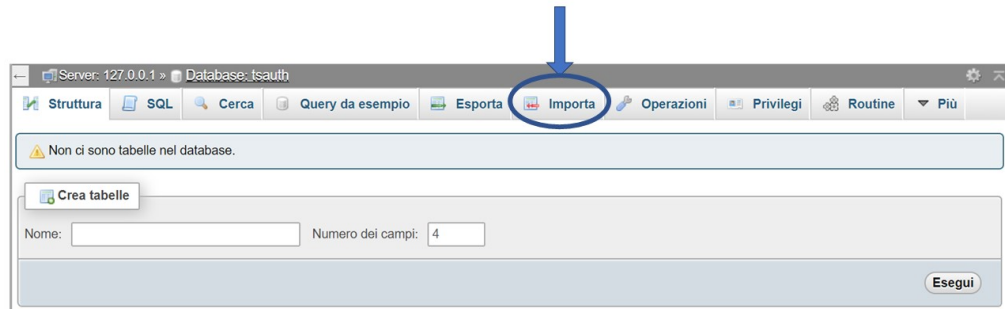


Figure A.5: Creation of the new database: set the name

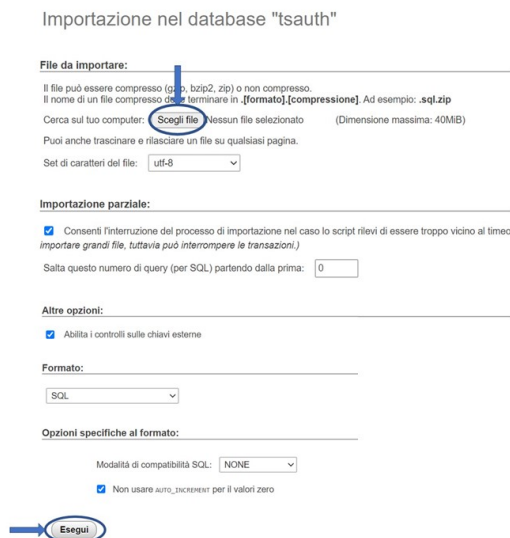


Figure A.6: Creation of the new database: import of the .sql file

- Go to the XAMPP folder (click on the "Explorer" button on the right side of the control panel);
- Open the "phpmyadmin" folder;
- Open the "config.inc.php" file;
- Write your password between the quotes, i.e. ' ' (Fig. A.10);
- Modify to *false* the last line (Fig. A.10);

Finally, in order to permit the connection to the database, the configuration file of the test must be modified:

- Search within "TSAuth_general" the file named "conf.php";
- Change the values that allow the access the own database, i.e. the password created for the database;

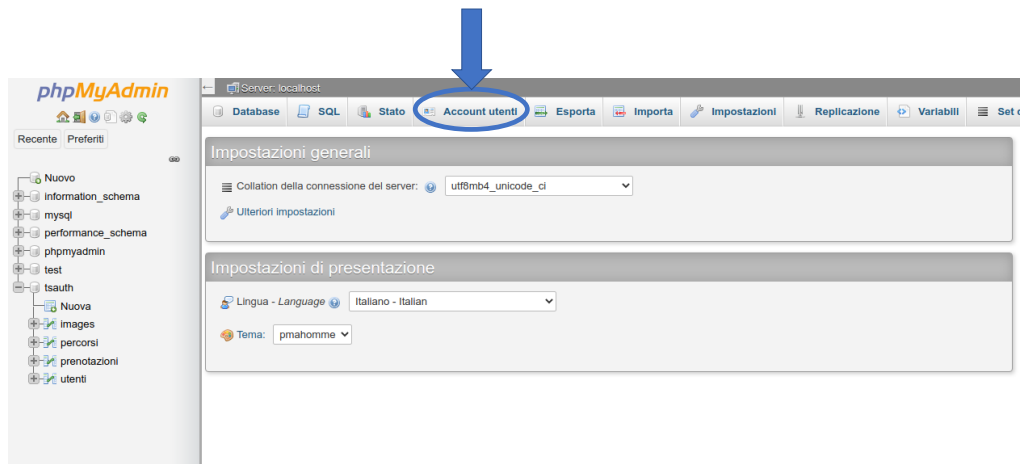


Figure A.7: Set a password: Overview of user accounts

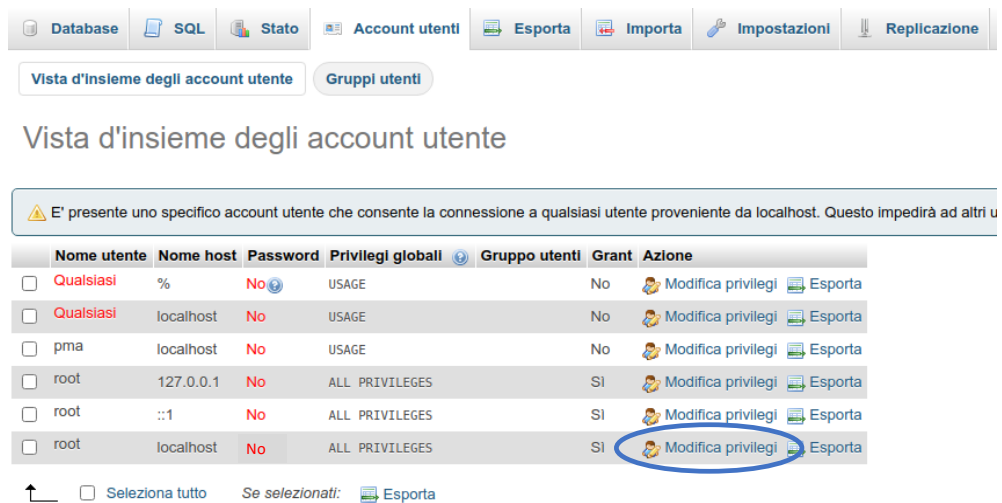


Figure A.8: Set a password: Edit privileges

- Save the file;

Now that the database has been created, the user can proceed with the test event at:
https://localhost/TSAuth_general/index.php

1.

Cambia password

Modifica privilegi: Account utente 'root'@'localhost'

2.

Cambia password

Modifica privilegi: Account utente 'root'@'localhost'

Nota: Stai cercando di modificare i privilegi dell'utente con cui sei collegato attualmente.

Cambia password

☐ Nessuna Password

☒ Password:

Inserisci: Strength: Good

Re-Inserisci:

Hash di password: Autenticazione MySQL nativa

Genera password:

Figure A.9: Set a password: Insert new password

```

<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * phpMyAdmin sample configuration, you can use it as base for
 * manual configuration. For easier setup you can use setup/
 *
 * All directives are explained in documentation in the doc/ folder
 * or at <https://docs.phpmyadmin.net/>.
 *
 * @package PhpMyAdmin
 */
declare(strict_types=1);

/**
 * This is needed for cookie based authentication to encrypt password in
 * cookie. Needs to be 32 chars long.
 */
$cfg['blowfish_secret'] = 'xampp'; /* YOU SHOULD CHANGE THIS FOR A MORE SECURE COOKIE AUTH! */

/**
 * Servers configuration
 */
$i = 0;

/**
 * First server
 */
$i++;
/* Authentication type */
$cfg['Servers'][$i]['auth type'] = 'config';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = '';
/* Server parameters */
// $cfg['Servers'][$i]['host'] = 'localhost';
$cfg['Servers'][$i]['compress'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = true;

/**
 * phpMyAdmin configuration storage settings.
 */
/* User used to manipulate with storage */
// $cfg['Servers'][$i]['controlhost'] = '';

```

Insert here your password, e.g 'pwd'

Write false instead of true

Figure A.10: Set a password: Modify the configuration file

Appendix B

Programmer manual

B.1 Development environment

The program was written within Eclipse Neon.3 (Release 4.6.3), through the Eclipse IDE for PHP Developers.

The specifications regarding the installation of the software components for the correct functioning of the prototype are described in the section “Installation manual” in the user manual [A.9](#).

The structure of the system is show in Fig. [B.1](#)

B.2 Global variables

In order to better comprehend the further sections and the whole functioning of the system, the global variables utilised in the entire project are described below.

`$_SESSION`

The `$_SESSION` superglobal variable is utilised in order to permit to pass different types of variables between all the pages of the project. In particular:

Session variable	Utilisation
<code>\$_SESSION['msg']</code>	It contains the messages to be printed in the log file or displayed in the client pages
<code>\$_SESSION['remai']</code>	It contains the user email in the registration phase
<code>\$_SESSION['pname']</code>	It contains the user email in the login phase
<code>\$_SESSION['username']</code>	It contains the user email when authenticated. If the user decides to change the username, this variable is modified. The change remains until logout, i.e. at the end of the session
<code>\$_SESSION['auth']</code>	It contains a boolean variable, which does not allow users to redirect to the page where the registration images are displayed from the url bar.
<code>\$_SESSION['log']</code>	It contains a boolean variable, which does not allow users to redirect to the page where the login images are displayed from the url bar.
<code>\$_SESSION['rimages']</code>	It contains the array of the registration images during the registration phase.
<code>\$_SESSION['logimages']</code>	It contains the array of the login images, which includes supplementary images randomly chosen, in addition to the registration images
<code>\$_SESSION['display']</code>	It is a counter for the images displayed

<code>\$_SESSION['err']</code>	It contains the user errors during the login phase
<code>\$_SESSION['refresh']</code>	It contains the number of page refresh
<code>\$_SESSION['train']</code>	It is a counter for the training sessions

\$_POST

The `$_POST` superglobal variable is utilised in order to collect form data from the HTML forms. All the actions performed are described in *actionform.php* (B.4).

B.2.1 Dimensions

The following variables indicate the dimensions of the image vectors and the thresholds to be respected. In view of a future possible change, they have been made global.

Variable	Utilisation
<code>\$MAX</code>	It is the length of the vector of the registration images
<code>\$LMAX</code>	It is the length of the vector of the login images, which include the registration images and additional random images
<code>\$TMAX</code>	It is the maximum number of training sessions
<code>\$EMAX</code>	It is the maximum number of errors allowed

B.3 Folders

In order to give a comprehensive description of the project, in this section the folders are briefly described.

- *CSS* folder
In this folder are contained all the CSS files utilised for the pages' graphic.
- *Images* folder
In this folder are contained all the images, which are used to compose the user secret. All the images are downloaded from Flickr, they are in the public domain and therefore manually edited with PowerPoint.
- *log* folder
In this folder is contained the log file. The file *myerrors.log* contains the messages captured by the `error_log()` function of the entire project (Fig. B.2).
- *Manual* folder
In this folder is contained the user manual in pdf format (see Appendix A).

B.4 Server side

***actionform.php* file**

This file contains the actions performed at the click on a button. The actions are described in the order in which they appear in the file, not according to the flow of operations requested by the user.

- **Sign In**

This action is triggered by the “SIGN IN” button in the *registration.php* page (B.5).

It checks in first instance the email format inserted by the user (B.4) and then if the user is already registered (B.4). In this latter case, it redirects to the Homepage, with the error message “The email is already registered! Please LOGIN.” Otherwise, the user is redirected to the *auth.php* page (B.5).

- **Auth**

This action is triggered by the direction button clicked by the user in the *images.php* page (B.5).

It checks if the direction clicked by the user, passed as a value of the global variable `$_POST['Auth']`, corresponds to the correct one associate with the image displayed (function `myDirection` B.4). In any case, the result is written in the log file. When `$_SESSION['rimages']` reaches the established size `$MAX`, it is shuffled in order to start the training session, where the images are displayed randomly.

- **TrainAuth**

This action is triggered by the direction button clicked by the user in the *training.php* page (B.5).

For `$TMAX` number of times, which represents the number of training sessions defined, all the images in `$_SESSION['rimages']` are displayed to the user.

For each image shown, the direction clicked by the user, passed as a value of the global variable `$_POST['TrainAuth']`, is checked by the function `myDirection` (B.4) and reported in the log file. Once all training sessions are completed, the `$_SESSION['rimages']` variable is transformed to a string and passed to the function “register” (B.4), in addition to the email inserted in the *registration.php* page.

- **Login**

This action is triggered by the “LOGIN” button in the *login.php* page (B.5).

It checks in first instance the email format inserted by the user (function `myEmail_format` B.4) and then if the user is already registered (function `myEmail_registered` B.4). If the user is not registered, it redirects to the Homepage, with the error message “The email is not registered! Please SIGN IN first.” and all the session variables set are unset. Otherwise, in the `$_SESSION['logimages']` both the images associated with the user and a number of random images are inserted. Finally, the `$_SESSION['logimages']` is shuffled and it redirects to the *login_images.php* page (B.5), where the images are displayed.

- **LoginAuth**

This action is triggered by the direction button clicked by the user in the *login_images.php* page (B.5).

For each image shown, the direction clicked by the user, passed as a value of the global variable `$_POST['LoginAuth']`, is checked by the function `myDirection` (B.4) and reported in the log file. In case of error the global variable `$_SESSION['err']` is incremented. When all the images in `$_SESSION['logimages']` have been displayed (i.e. `$_SESSION['display']` reaches the value of `$LMAX`), it recalls the function “login” (B.4), with the parameters `$_SESSION['pname']`, which correspond to the email inserted in the *login.php* page and the `$_SESSION['err']` variable.

- **Logout**

This action is triggered by the “Logout” button clicked by the user in the *ppage.php* page (B.5) and recalls the function “myLOGOUT()” (B.4).

- **Book**

This action is triggered by the “Book your trip” button clicked by the user in the *ppage.php* page (B.5) and redirects to the *reservation.php* page (B.5), with the message “Book”.

- **End**

This action is triggered by the “End” button clicked by the user in the *reservation.php* page

(B.5).

In first instance, it checks if the departure (i.e. `$_POST['from']`) and the arrival (i.e. `$_POST['to']`) points have been selected. Then, it checks if the path is possible recalling the function “myPossible” (B.4). In case of success, it updates the database recalling the function “myResearch” (B.4).

- **DeleteTrip**

This action is triggered by the “Delete your trip” button clicked by the user in the *ppage.php* page (B.5) and recalls the function “myDelete()” (B.4).

- **AccountDelete**

This action is triggered by the “Delete account” button clicked by the user in the *ppage.php* page (B.5) and recalls the function “myDeleteAccount()” (B.4).

- **Help**

This action is triggered by the “?” button clicked by the user and redirects to the page specified as `$_POST['Help']` value.

- **UChange**

This action is triggered by the “Change Username” button clicked by the user in the *ppage.php* page (B.5) and redirects to the *change.php* page (B.5).

- **Change**

This action is triggered by the “CHANGE” button clicked by the user in the *change.php* page (B.5) and set the global variable `$_SESSION['username']` with the value of `$_POST['change']`. Finally it redirects to the personal page, where the username is shown instead of the email.

analytics file

This file contains the javaScripts needed to allow the inspection of the site by different analytics sites, such as Google Analytics, Hotjar and Inspectlet.

myfunctions.php file

This file contains all the function needed by the system in order to correctly work.

- **userLoggedIn()**

This function controls that a user have executed the log in. It is inserted into the *ppage.php*

- **myRedirect(\$page="", \$msg="")**

This function is recalled by the other functions in order to redirect to different pages. The two parameters passed indicates the page where to be redirected and the message to be written in the log file. Furthermore, if the user has successfully registered or logged in, the function appends the user’s email to the beginning of the message to be printed in the log file. Otherwise, it has to be specified in the string passed as “msg” parameter.

- **myDestroySession()**

This function destroys the session, including the cookie set and the `$_SESSION[]` global variable. The function redirects to the Homepage, with no messages to be displayed to the user.

- **dbConnect()**

This function permits to query the database. It refers to the variables set in the *config.php* file.

- **myhttps()**

This function redirects on HTTPS.

- ***cookieon()***
This function controls if the cookie associated with the user has been not set or has expired. In both cases it is not valid and therefore the session is destroyed.
- ***set_cookie()***
This function set the cookie associated with the user who successfully registered or logged in. An idle time limit of 10 minutes is set.
- ***myLOGOUT()***
This function destroys the session when the “Logout” button in the personal page is clicked.
- ***myEmail_format(\$email)***
This function controls the format of the email insert in the registration page and in the login page, passed as parameter. It deletes spaces, ”wrap” and more at the ends of the string and checks the presence of a single @ in the string. Furthermore, it controls for additional ”dangerous” characters, such as comma, semicolon, exclamation and question marks.
- ***myEmail_registered(\$db,\$email)***
This function controls if the email inserted is already in the users’ database. The parameters to be passed are the connection to the database (i.e. connection returned from the *dbConnect()* function) and the email of the user. It returns “true” if the user is present in the database, false otherwise.
- ***myImages(\$email)***
This function retrieves the images associated with the user. In order to query the database, the email of the user has to be passed as parameter. The function returns the array where are listed the images, separated by a comma. In case of error, the function redirects to the Homepage, with the error message to be displayed to the user: “No secret registered for this user. ”. In this case, in the log file “no secret found” is written.
- ***register(\$email, \$secre)***
This function inserts the user’s email and the associated set of images into the database. In order to construct the query, the email and the string which lists the images of the user have to be passed as parameters. Once the insert query has been executed, a series of session variables are set. Finally, it redirects to the *questionnaire.php* page, with the message “Registration completed”, which is written in the log file.
In case of errors the function redirects to the Homepage, with the error message “Registration failed.”
- ***login(\$email, \$err)***
This function controls if the errors committed by the user during the login phase exceed the threshold “\$EMAX”. The error parameter correspond to the global variable \$_SESSION[‘err’], set in the *login_images.php* file and incremented in the *actionform.php* file and the *login_images.php* file.
If the login has been successfully completed a series of session variables are set and the number of errors committed are reported in the log file. Otherwise, the function redirects to the Homepage, with the error message “LOGIN FAILED.” Finally, it redirects to the *questionnaire.LOGIN.php* file.
- ***myDirection(\$im)***
This function permits to retrieve the direction of the arrow of the image passed as parameter from the database. In case of error the function redirects to the Homepage, with the error message “DIRECTION NOT FOUND.” and report the error in the log file.
- ***myPossible(\$from,\$to)***
This function controls if the departure point precedes the arrival point. In this case, the path inserted is not valid and the function redirects the user to the *reservation.php* page, with the associated message “IMPOSSIBLE PATH. Try again”, which is also written in the log file.

- ***myResearch(\$from, \$to, \$p)***

This function permits the user to book a trip from predefined paths. It controls in first instance if the number of passengers inserted by the user exceed the maximum number of passengers of the minibus. In this case, the function redirects to the same page with the error message “REQUEST DENIED. There is not a place for everyone.”, which is also reported in the log file.

If the number of passengers for the specified path does not exceed the maximum, the path is inserted into the ‘prenotazioni’ table in the database and the ‘percorsi’ table is updated, with the total final number of passengers. If the queries are successfully committed, the function redirects to the *ppage.php* page, with the message “Record successfully updated.”. In case of error, the function redirects to the same page with the specified error message.

- ***myDelete()***

This function deletes the trip booked by the user, updating the involved database tables. If the queries are successfully committed, the function redirects to the *ppage.php* page, with the message “RESERVATION SUCCESSFULLY DELETED.”. In case of error, the function redirects to the *ppage.php* page, with the corresponding error message.

- ***myDeleteAccount()***

This function deletes the user from the entire database, including the trip reservations done in a previous moment. If the queries are successfully committed, the function redirects to the Homepage, with the message “Account SUCCESSFULLY DELETED.”; otherwise it redirects to the *ppage.php* page, with the corresponding error message.

B.5 Client side

In this section the description of the files follows the the order of actions requested to the user to successfully complete the test.

index.php

This page is the Homepage. It contains the menu where to start both the registration and the login, in addition to the link to the final questionnaire, which is a Google format questionnaire and the Help button, which permits to consult the user manual.

In this page the main errors are displayed through the `$_SESSION['msg']` variable.

registration.php

In this page, the user is required to enter the email and click the “SIGN IN” button, which is a submit type of button with `method=“post”`. The triggered action is described in the file *actionform.php* (B.4). In addition the “Cancel” and the “Back” buttons are inserted to facilitate the cancellation of the entire form and the navigation.

auth.php

In this page, the user is notified that the registration phase is about to begin. It includes the “START!” and the “Back” buttons, which redirects respectively to the *images.php* page and the *registration.php* page.

In this page is inserted a control on the `$_SESSION['remail']` value, set in the *Sign In* action (B.4), in order to not permit to access this page from the address bar.

images.php

In this page the images to be associated with the user are randomly selected from the “Images” folder. The images are inserted into the global variable `$_SESSION['rimages']`, initialized the first time the *images.php* page is accessed. In order to ensure the correct sequence of actions that the user must perform, a control on the variable `$_SESSION['auth']` is executed (set in B.4): if the user accesses this page without first entering the email (i.e. accessing the registration page), the function redirects to the Homepage with the error message “Something went wrong during registration. Complete correctly the steps to registration.”.

The submit buttons in the form trigger the actions described in the file *actionform.php* (B.4).

training.php

In this page a series of global session variables are set in order to permits the correct functioning of the training phase. In addition to the verification of the variable `$_SESSION['reemail']`, in the same manner as in the *images.php* page(B.5), the `$_SESSION['display']` and the `$_SESSION['refresh']` variables are initialised. The variable `$_SESSION['refresh']` indicates the number of times the page is refreshed: in fact, after 5 seconds of inactivity, the page is reloaded with a new different image and the user’s error is reported in the log file, with the message “TRAINING_page refreshed” and the last image displayed. The `$_SESSION['display']` variable allows to iterate on the vector of images of the registration phase (i.e. `$_SESSION['rimages']`). The `$_SESSION['train']` variable represent the number of sessions; if the user commits a \$MAX number of errors, a supplementary training session is added, decrementing this variable.

The submit buttons in the form trigger the actions described in the file *actionform.php* (B.4).

questionnaire.php

This page include the Google form questionnaire “HOW DO YOU FEEL”, regarding the registration phase, which permits to collect data about the emotional state of the user immediately after the completion of the task. In this manner it is possible to gather information to be compared with the data acquired through objective metrics, such as eye-tracking and heart rate variability.

ppage.php

This page is an auxiliary page, which is not it essential for the purpose of the test. Controls on the `$_SESSION['log']` variable and on the cookie are executed, in order to not allow a user to reach the personal page through the address bar if not authenticated.

The submit buttons in the form trigger the actions described in the file *actionform.php*, respectively “Book your trip” (B.4), “Delete your trip” (B.4), “Change Username” (B.4), “Delete account” (B.4), “Logout” (B.4).

reservation.php

This page allows the user to book a trip from for predetermined routes. In the same manner as the previously described files, controls are executed in order to not permit unauthorised access to the page (i.e. on the `$_SESSION['log']` variable and the cookie). The submit button “End” in the form triggers the actions described in the file *actionform.php* (B.4).

change.php

This page allows the user to change the username displayed in the personal page. In the same manner as the previously described files, controls are executed in order to not permit unauthorised access to the page (i.e. on the `$_SESSION['log']` variable and the cookie). The submit button “Change” in the form triggers the actions described in the file *actionform.php* (B.4).

login.php

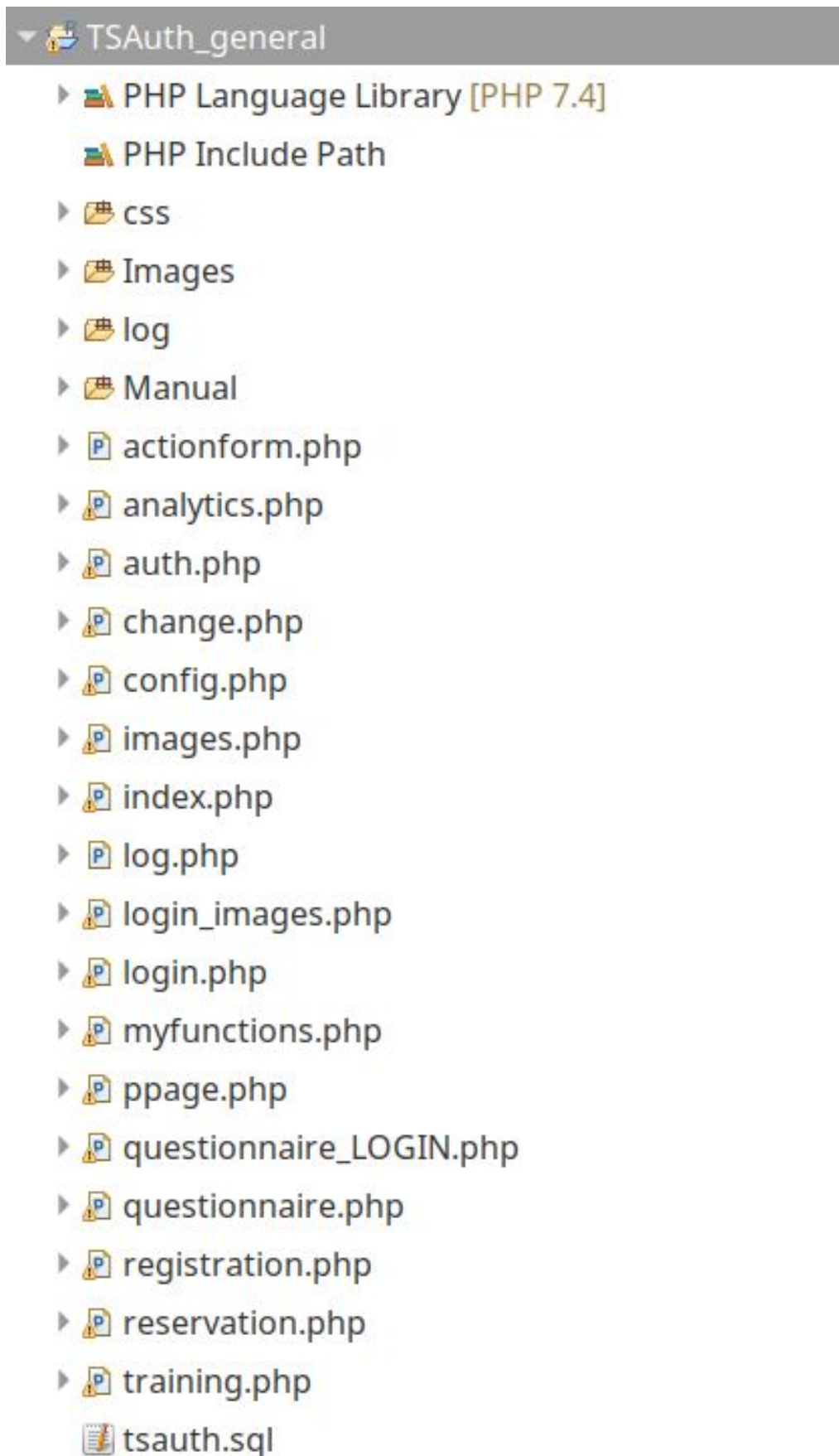
In this page, the user is required to enter the email (not the eventually changed username) and click the “LOGIN” button, which is a submit type of button with `method=“post”`. The triggered action is described in the file *actionform.php* (B.4). Furthermore, the array to be displayed to the user in the login phase, i.e. `$_SESSION['logimages']`, is initialised. The submit button “LOGIN” in the form triggers the actions described in the file *actionform.php* (B.4).

login_images.php

In this page the set of images for the login are displayed from the global variable `$_SESSION['logimages']`. In order to ensure the correct sequence of actions that the user must perform, a control on the variable `$_SESSION['logimages']` is executed (set in B.5): if the user accesses this page without first entering the email (i.e. accessing the login page), the function redirects to the Homepage with the error message “Something went wrong during the login. Complete correctly the steps.”. The global variables `$_SESSION['err']` and `$_SESSION['refresh']` permits to control the number of user’s errors. Once the three errors threshold has been exceeded, the user is directly sent back to the Homepage. The submit buttons, named “Auth”, in the form, trigger the actions described in the file *actionform.php* (B.4).

questionnaire_LOGIN.php

This page include the Google form questionnaire “HOW DO YOU FEEL”, concerning the login phase, which permits to collect data of the emotional state of the user immediately after the completion of the task. In this manner it is possible to gather information to be compared with the data acquired through objective metrics, such as eye-tracking and heart rate variability.



```
[19-Jun-2020 13:56:31 Europe/Berlin] albertorobustelli@yahoo.it ERRORS COMMITTED during login: 1  
[19-Jun-2020 13:56:31 Europe/Berlin] albertorobustelli@yahoo.it LOGIN SUCCESS with_errors: 1  
[19-Jun-2020 13:57:58 Europe/Berlin] albertorobustelli@yahoo.it First_session  
[19-Jun-2020 13:58:26 Europe/Berlin] albertorobustelli@yahoo.it Account SUCCESSFULLY DELETED.
```

Figure B.2: Log file sample

Bibliography

- [1] G. Mathew and S. Thomas, “A Novel Multifactor Authentication System Ensuring Usability and Security”, ArXiv, abs/1311.4037, 2013, pp. 35-41, DOI [10.5121/ijstpm.2013.2503](#)
- [2] C. Katsiniot, M. Belk, C. Fidas, N. Avouris and G. Samaras “Security and Usability in Knowledge-based User Authentication: A Review”, PCI ‘16: 20th Pan-Hellenic Conference on Informatics, Patras (Greece), November, 2016, pp. 1-6, DOI [10.1145/3003733.3003764](#)
- [3] M. H. Barkadehi, M. Nilashia, O. Ibrahim, A. Z. Fardi and S. Samad, “Authentication Systems: A Literature Review and Classification”, Telematics and Informatics, Vol. 35, No. 5, March 2018, pp. 1491-1511, DOI [10.1016/j.tele.2018.03.018](#)
- [4] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication”, Proceedings of the IEEE, Vol. 91, No. 12, December 2003, pp. 2019-2040, DOI [10.1109/JPROC.2003.819611](#)
- [5] A. Conklin, G. Dietrich, D. Walz, “Password-based authentication: a system perspective”, HICSS: 37th Annual Hawaii International Conference on System Sciences, Big Island, HI (USA), January 5-8, 2004, pp. 1-6, DOI [10.1109/HICSS.2004.1265412](#)
- [6] A. A. Kaur and K. K. Mustafa, “A Critical appraisal on Password based Authentication”, I. J. Computer Network and Information Security, January 2019, pp. 47-61, DOI [10.5815/ijcnis.2019.01.05](#)
- [7] L. Bosnjak and B. Brumen, “Examining Security and Usability Aspects of Knowledge-based Authentication Methods”, MIPRO: 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija (Croatia), May 20-24, 2019, pp. 1181-1186, DOI [10.23919/MIPRO.2019.8756655](#)
- [8] C. Herley, P. C. van Oorschot and A. S. Patrick, “Passwords: If We’re So Smart, Why Are We Still Using Them?” FC 2009: International Conference on Financial Cryptography and Data Security, Accra Beach (Barbados), February 23-26, 2009, pp. 230-237, DOI [10.1007/978-3-642-03549-4_14](#)
- [9] A. De Luca, R. Weiss and H. Drewes, “Evaluation of eye-gaze interaction methods for security enhanced PIN-entry”, OZCHI ’07:19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces, Adelaide (Australia), November 28-30, 2007, pp. 199-202, DOI [10.1145/1324892.1324932](#)
- [10] A. De Luca, K. Hertzschuch and H. Hussmann, “ColorPIN: securing PIN entry through indirect input”, CHI ’10: CHI Conference on Human Factors in Computing Systems, Atlanta, Georgia (USA), April 10-15, 2010, pp. 1103-1106, DOI [10.1145/1753326.1753490](#)
- [11] A. Gutmann, M. Volkamer and K. Renaud, “Memorable and Secure: How Do You Choose Your PIN?” in the book “HAISA” edited by Springer, Berlin, Heidelberg, 2016, pp. 156-166
- [12] K. Renaud, P. Mayer, M. Volkamer and J. Maguire, “Are graphical authentication mechanisms as strong as passwords?”, FedCSIS 2013: Federated Conference on Computer Science and Information Systems, Krakow (Poland), September 8-11, 2013, pp. 837-844
- [13] R. Biddle, S. Chiasson and P.C. Van Oorschot, “Graphical passwords: Learning from the first twelve years”, ACM Computing Surveys (CSUR), Vol. 44, No. 4, August 2012, Article No. 19, DOI [10.1145/2333112.2333114](#)
- [14] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system”, Int. J. Human-Computer Studies, Vol. 63, July 2005, pp. 102-127, DOI [10.1016/j.ijhcs.2005.04.010](#)

- [15] J. H. Huh, H. Kim, R. B. Bobba, M. N. Bashir and K. Beznosov, "On the Memorability of System-generated PINs: Can Chunking Help?", SOUPS '15: 11th USENIX Conference on Usable Privacy and Security, Ottawa (Canada), July 2015, pp. 197-209, DOI [10.5555/3235866.3235883](https://doi.org/10.5555/3235866.3235883)
- [16] P. Mayer, M. Volkamer and M. Kauer, "Authentication Schemes - Comparison and Effective Password Spaces" in the book "Information Systems Security" edited by A. Prakash, R. Shyamasundar, Springer, Cham, 2014, pp. 204-225 DOI [10.1007/978-3-319-13841-1_12](https://doi.org/10.1007/978-3-319-13841-1_12)
- [17] R. Biddle, S. Chiasson and P.C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years", ACM Computing Surveys (CSUR), Vol. 44, No. 4, September 2012, pp. 1-41, DOI [10.1145/2333112.2333114](https://doi.org/10.1145/2333112.2333114)
- [18] S. Frischat, "The next generation of USB security tokens", Card Technology Today, Vol. 20, No. 6, 2008, pp. 10-11, DOI [10.1016/S0965-2590\(08\)70153-1](https://doi.org/10.1016/S0965-2590(08)70153-1)
- [19] U. Trottmann, "NFC-possibilities and risks", Network Architectures and Services, Vol. 35, February 2013, pp. 35-42, DOI [10.2312/NET-2013-02-1.05](https://doi.org/10.2312/NET-2013-02-1.05)
- [20] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC Devices: Security and Privacy", ARES: 3rd International Conference on Availability, Reliability and Security, Barcelona (Spain), March 4-7, 2008, pp. 642-647, DOI [10.1109/ARES.2008.105](https://doi.org/10.1109/ARES.2008.105)
- [21] F. Aloul, S. Zahidi and W. El-Hajj, "Two factor authentication using mobile phones", ACS/IEEE: International Conference on Computer Systems and Applications, Rabat (Morocco), May 10-13, 2009, pp. 641-644, DOI [10.1109/AICCSA.2009.5069395](https://doi.org/10.1109/AICCSA.2009.5069395)
- [22] M. Aizomai, Audun Josang, A. McCullagh and E. Foo, "Strengthening SMS-Based Authentication through Usability", ISPA: International Symposium on Parallel and Distributed Processing with Applications, Sydney, NSW (Australia), December 10-12, 2008, pp. 683-688, DOI [10.1109/ISPA.2008.57](https://doi.org/10.1109/ISPA.2008.57)
- [23] B. Maciej, E.F. Imed and M. Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment", IEEE Access, Vol. 7, October 2019, pp. 157185 - 157199, DOI [10.1109/ACCESS.2019.2948922](https://doi.org/10.1109/ACCESS.2019.2948922)
- [24] D. van Thanh, I. Jorstad, T. Jonvik and D. van Thuan, "Strong authentication with mobile phone as security token", MASS: 6th International Conference on Mobile Adhoc and Sensor Systems, Macau (China), October 12-15, 2009, pp. 777-782, DOI [10.1109/MOB-HOC.2009.5336918](https://doi.org/10.1109/MOB-HOC.2009.5336918)
- [25] B. Sodhi, "Transferring Data via Dropped Calls", WICON: 8th International Wireless Internet Conference, Lisbon (Portugal), November 13-14, 2014, pp. 229-234, DOI [0.1007/978-3-319-18802-7_31](https://doi.org/10.1007/978-3-319-18802-7_31)
- [26] Y. Albayram, M.M.H Khan, A. Bamis, S. Kentros, N. Nguyen and R. Jiang "Designing challenge questions for location-based authentication systems: a real-life study", Human-centric Computing and Information Sciences, Vol. 5, No. 17, 2015, pp. 1-28, DOI [10.1186/s13673-015-0032-3](https://doi.org/10.1186/s13673-015-0032-3)
- [27] D. Weinshall, "Cognitive authentication schemes safe against spyware", S&P'06: IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA (USA), May 21-24, 2006, pp. 1-6, DOI [10.1109/SP.2006.10](https://doi.org/10.1109/SP.2006.10)
- [28] E. Hayashi and N. Christin, "Use Your Illusion: Secure Authentication Usable Anywhere", SOUPS '08: The fourth Symposium on Usable Privacy and Security, Pittsburgh, PA (USA), July 23-25, 2008, pp. 35-45, DOI [10.1145/1408664.1408670](https://doi.org/10.1145/1408664.1408670)
- [29] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: a tool for information security", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, June 2006, pp. 125-143, DOI [10.1109/TIFS.2006.873653](https://doi.org/10.1109/TIFS.2006.873653)
- [30] P. Varchol and D. Levicky, "Using of Hand Geometry in Biometric Security Systems", Radioengineering, Vol. 16, No. 4, January 2007, pp. 82-87
- [31] N. Pavesic, S. Ribaric and D. Ribaric, "Personal authentication using hand-geometry and palmprint features-the state of the art", Hand, Vol. 11, January 2004, pp. 1-10, DOI [10.1.1.93.8771](https://doi.org/10.1.1.93.8771)
- [32] M. Dewangan and L. K. B. Bhaiya, "Palm-Print Based Biometric Authentication Systems - A Review", International Journal of Science and Research (IJSR), Vol. 3, No. 5, May 2014, pp. 400-405

- [33] I. M. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages and future development: a review", *International Journal of Scientific & Technology Research*, Vol. 4, No. 12, December 2015, pp. 285-289
- [34] V.P. Kshirsagar, M.E. Gaikwad and M.R. Baviskar, "Face recognition using Eigenfaces", ICCRD: 3rd International Conference on Computer Research and Development, Shanghai (China), March 11-13, 2011, pp. 302-306, DOI [10.1109/ICCRD.2011.5764137](https://doi.org/10.1109/ICCRD.2011.5764137)
- [35] Face Recognition Technology Whitepaper, <https://www.fingertec.com/companyprofile/development/wp-facerecognition.html>
- [36] R.P. Wildes, "Iris recognition: an emerging biometric technology", *Proceedings of the IEEE*, Vol. 85, No. 9, September 1997, pp. 1348-1363, DOI [10.1109/5.628669](https://doi.org/10.1109/5.628669)
- [37] J. Daugman, "Chapter 25 - How Iris Recognition Works" in the book "The Essential Guide to Image Processing" edited by Al Bovik, Academic Press, 2009, pp. 715-739, DOI [10.1016/B978-0-12-374457-9.00025-1](https://doi.org/10.1016/B978-0-12-374457-9.00025-1)
- [38] Iris ID technology included in Ultra Electronics' tactical information system for military application, <https://www.sourcesecurity.com/news/iris-id-technology-included-ultra-electronics-tactical-information-system-military-application-23178.html>
- [39] A. Ross, "A prototype hand geometry-based verification system", AVBPA: 2nd International Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C. (USA), March 22-24, 1999, pp. 166-171
- [40] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification", *International Journal of Biometrics*, Vol. 1, No. 1, June 2008, pp. 81-113 DOI [10.1504/IJBM.2008.018665](https://doi.org/10.1504/IJBM.2008.018665)
- [41] Signature Verification/Signature Authentication (SIGNificant Biometric Server), https://www.icon-uk.net/signature_biometrics.html
- [42] The new StepOver duraSign Pad 10.0 signature pad, <https://www.pressebox.com/pressrelease/stepover-gmbh/The-new-StepOver-duraSign-Pad-10-0-signature-pad/boxid/928227>
- [43] A. Ross and A. K. Jain, "Human recognition using biometrics: an overview.", *Annales Des Télécommunications*, Vol. 62, 2007, pp. 11-35, DOI [10.1007/BF03253248](https://doi.org/10.1007/BF03253248)
- [44] J. Linden, R. Marquis, S. Bozza and F. Taronia, "Dynamic signatures: A review of dynamic feature variation and forensic methodology", *Forensic Science International*, Vol. 291, October 2018, pp. 216-229, DOI [10.1016/j.forsciint.2018.08.021](https://doi.org/10.1016/j.forsciint.2018.08.021)
- [45] J. Kim, H. Kim and P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection", *Applied Soft Computing*, Vol. 62, January 2018, pp. 1077-1087, DOI [10.1016/j.asoc.2017.09.045](https://doi.org/10.1016/j.asoc.2017.09.045)
- [46] User Verification based on Keystroke Dynamics: Python code, <https://appliedmachinelearning.blog/2017/07/26/user-verification-based-on-keystroke-dynamics-python-code/>
- [47] A. A. E. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics", *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 3, 2007, pp. 165-179, DOI [10.1109/TDSC.2007.70207](https://doi.org/10.1109/TDSC.2007.70207)
- [48] The Mouse That Knows You, <https://www.hood.edu/discover/stories/mouse-knows-you>
- [49] Viewing the Mouse Tracks You Leave Behind, <https://bits.blogs.nytimes.com/2010/02/16/viewing-the-mouse-tracks-you-leave-behind/>
- [50] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach and A. Schlarb, "User identity verification via mouse dynamics", *Information Sciences*, Vol. 201, 15 October 2012, pp. 19-36, DOI [10.1016/j.ins.2012.02.066](https://doi.org/10.1016/j.ins.2012.02.066)
- [51] Speechlog voice authentication, <https://www.globitel.com/globitel-speechlog-voice-authentication/pr-banner-voice-print-01/>
- [52] The benefits of voice identification, <https://www.argustrueid.com/voice-identification/>
- [53] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification", *IEEE Access*, Vol. 7, December 2018, pp. 5994 - 6009, DOI [10.1109/ACCESS.2018.2861111](https://doi.org/10.1109/ACCESS.2018.2861111)

- 10.1109/ACCESS.2018.2889996
- [54] IPI partners with Aculab on voice biometrics, <https://www.planetbiometrics.com/article-details/i/10733/desc/ipi-partners-with-aculab-on-voice-biometrics/>
 - [55] Y. Singh, S. Singh and A. Ray, "Bioelectrical Signals as Emerging Biometrics: Issues and Challenges", *ISRN Signal Processing*, Vol. 2012, July 2012, pp. 1-13, DOI [10.5402/2012/712032](https://doi.org/10.5402/2012/712032)
 - [56] F. Sufi, I. Khalil and J. Hu, "ECG-Based Authentication" in the book "Handbook of Information and Communication Security", Springer, Berlin, Heidelberg 2010, pp. 309-331, DOI [10.1007/978-3-642-04117-4_17](https://doi.org/10.1007/978-3-642-04117-4_17)
 - [57] S. Keshishzadeh, A. Fallah and S. Rashidi, "Improved EEG based human authentication system on large dataset", *ICEE: 24th Iranian Conference on Electrical Engineering*, Shiraz (Iran), May 10-12, 2016, pp. 1165-1169, DOI [10.1109/IranianCEE.2016.7585697](https://doi.org/10.1109/IranianCEE.2016.7585697)
 - [58] 81% Of Company Data Breaches Due To Poor Passwords, <https://bnd.nd.gov/81-of-company-data-breaches-due-to-poor-passwords/>
 - [59] Get smarter with passwords, <https://www.cyber.gov.au/news/get-smarter-with-passwords>
 - [60] M. N. Al-Ameen, M. Wright and S. Scielzo, "Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues", *CHI '15: CHI Conference on Human Factors in Computing Systems*, Seoul (Republic of Korea), April 2015, pp. 2315-2324, DOI [10.1145/2702123.2702241](https://doi.org/10.1145/2702123.2702241)
 - [61] P. Mayer, M. Volkamer and M. Kauer, "Authentication Schemes - Comparison and Effective Password Spaces", *ICISS 2014: International Conference on Information Systems Security*, Hyderabad (India), December 16-20, 2014, pp. 204-225, DOI [10.1007/978-3-319-13841-1_12](https://doi.org/10.1007/978-3-319-13841-1_12)
 - [62] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. M. Vidas, L. Bauer, N. Christin and L. F. Cranor, "Correct horse battery staple: exploring the usability of system-assigned passphrases", *SOUPS '12: 8th Symposium on Usable Privacy and Security*, Washington D.C. (USA), July 2012, pp. 1-20, DOI [10.1145/2335356.2335366](https://doi.org/10.1145/2335356.2335366)
 - [63] R. Alomari, M. V. Martin, S. MacDonald, A. Maraj, R. Liscano and C. Bellman, "Inside out - A study of users' perceptions of password memorability and recall", *Journal of Information Security and Applications*, Vol. 47, August 2019, pp. 223-234, DOI [10.1016/j.jisa.2019.05.009](https://doi.org/10.1016/j.jisa.2019.05.009)
 - [64] E. L.G. Legge, C. R. Madan, E. T.Ng and J. B. Caplan, "Building a memory palace in minutes: Equivalent memory performance using virtual versus conventional environments with the Method of Loci", *Acta Psychologica*, Vol. 141, No. 3, November 2012, pp. 380-390, DOI [10.1016/j.actpsy.2012.09.002](https://doi.org/10.1016/j.actpsy.2012.09.002)
 - [65] T. Dalgleish, L. Navrady, E. Bird, E. Hill, B. D. Dunn and A. Golden, "Method-of-Loci as a Mnemonic Device to Facilitate Access to Self-Affirming Personal Memories for Individuals With Depression", *SAGE journals*, Vol. 1, No. 2, February 2013, pp. 156-162, DOI [10.1177/2167702612468111](https://doi.org/10.1177/2167702612468111)
 - [66] Use The Memory Palace Technique For Exams, <http://www.oldschoolasc.com/use-the-memory-palace-technique-for-exams.html>
 - [67] Increase Memory with The Linking Method, <https://www.mind-expanding-techniques.net/memory-strategies-how-to-improve-your-memory/linking-method/>
 - [68] A. Kriston, "The importance of memory training in interpretation", *Professional communication and translation studies*, Vol. 5, No. 1-2, 2012, pp. 79-86
 - [69] The Link Method: An Image-Based Technique for Memorizing Lists, <https://www.memory-improvement-tips.com/link-method.html>
 - [70] Forgetfulness - 7 types of normal memory problems, <https://www.health.harvard.edu/mind-and-mood/forgetfulness-7-types-of-normal-memory-problems>
 - [71] D. L. Schacter, C. Y. P. Chiu and K. N. Ochsner, "Implicit Memory: A Selective Review", *Annual Review of Neuroscience*, Vol. 16, No. 1-2, March 1993, pp. 159-182, DOI [10.1146/annurev.ne.16.030193.001111](https://doi.org/10.1146/annurev.ne.16.030193.001111)
 - [72] P. Gupta and N.J. Cohen, "Theoretical and Computational Analysis of Skill Learning, Repetition Priming, and Procedural Memory", *Annual Review of Neuroscience*, Vol. 109, No. 2, April 2002, pp. 401-448, DOI [10.1037/0033-295X.109.2.401](https://doi.org/10.1037/0033-295X.109.2.401)

- [73] F. Gobet, P. C. R. Lane, S. Croker, P. C-H. Cheng, G. Jones, I. Oliver and J. M. Pine, "Chunking mechanisms in human learning", *Trends in Cognitive Sciences*, Vol. 5, No. 1, June 2001, pp. 236-243, DOI [10.1016/S1364-6613\(00\)01662-4](https://doi.org/10.1016/S1364-6613(00)01662-4)
- [74] D. S. Carstens, L. C. Malone and P. R. Mccauley-Bell, "Applying Chunking Theory in Organizational Password Guidelines", *Journal of Information, Information Technology, and Organizations*, Vol. 1, 2006, pp. 97-113, DOI [10.28945/150](https://doi.org/10.28945/150)
- [75] A. Hollingworth and J. M. Henderson, "Accurate Visual Memory for Previously Attended Objects in Natural Scenes", *Journal of Experimental Psychology*, Vol. 28, No. 1, 2002, pp. 113-136, DOI [10.1037//0096-1523.28.1.113](https://doi.org/10.1037//0096-1523.28.1.113)
- [76] M. Castelhana and J. M. Henderson, "Incidental visual memory for objects in scenes", *Visual Cognition*, Vol. 12, No. 6, August 2005, pp. 113-136, DOI [10.1080/13506280444000634](https://doi.org/10.1080/13506280444000634)
- [77] M. M. Chun, "Contextual cueing of visual attention", *Trends in Cognitive Sciences*, Vol. 4, No. 5, May 2000, pp. 170-178, DOI [10.1016/s1364-6613\(00\)01476-5](https://doi.org/10.1016/s1364-6613(00)01476-5)
- [78] C. Castelluccia, M. Duermuth, M. Golla and F. Deniz, "Towards Implicit Visual Memory-Based Authentication", *NDSS '17: Network and Distributed System Security Symposium*, San Diego (USA), February 26 - March 1, 2017, pp. 1-15, DOI [10.14722/ndss.2017.23292](https://doi.org/10.14722/ndss.2017.23292)
- [79] MooneyAuth: Implicit Authentication, <https://www.mooneyauth.org/static/index.php>
- [80] Z. Joudaki, J. Thorpe and M. V. Martin, "Enhanced Tacit Secrets: System-assigned passwords you can't write down, but don't need to", *International Journal of Information Security*, Vol. 18, May 2018, pp. 239-255, DOI [10.1007/s10207-018-0408-2](https://doi.org/10.1007/s10207-018-0408-2)
- [81] J. W. Krakauer and R. Shadmehr, "Consolidation of motor memory", *Trends in Cognitive Sciences*, Vol. 29, No. 1, January 2006, pp. 58-64, DOI [10.1016/j.tins.2005.10.003](https://doi.org/10.1016/j.tins.2005.10.003)
- [82] F. Ebbers and P. Brune, "The Authentication Game - Secure User Authentication by Gamification?", *CAiSE 2016: International Conference on Advanced Information Systems Engineering*, Ljubljana (Slovenia), June 13-14, 2016, pp. 101-115, DOI [10.1007/978-3-319-39696-5_7](https://doi.org/10.1007/978-3-319-39696-5_7)
- [83] H. Bojinov, D. J. Sanchez, P. Reber, D. Boneh and P. D. Lincoln, "Neuroscience meets cryptography: Designing crypto primitives secure against rubber hose attacks", *USENIX Security '12: 21st USENIX conference on Security symposium*, Bellevue, WA (USA), August 8-10, 2012 pp. 129-141, DOI [10.5555/2362793.2362826](https://doi.org/10.5555/2362793.2362826)
- [84] D. J. Sanchez, E. W. Gobel and P. J. Reber, "Performing the unexplainable: implicit task performance reveals individually reliable sequence learning without explicit knowledge", *Psychonomic Bulletin & Review*, Vol. 17, No. 6, December 2010, pp. 790-796, DOI [10.3758/PBR.17.6.790](https://doi.org/10.3758/PBR.17.6.790)
- [85] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems", *Proceedings of the IEEE*, Vol. 63, No. 9, September 1975, pp. 1278 - 1308, DOI [10.1109/PROC.1975.9939](https://doi.org/10.1109/PROC.1975.9939)
- [86] D. Balfanz, G. Durfee, D. K. Smetters and R. E. Grinter, "In search of usable security: five lessons from the field", *IEEE Security & Privacy*, Vol. 2, No. 5, October 2004, pp. 19-24, DOI [10.1109/MSP.2004.71](https://doi.org/10.1109/MSP.2004.71)
- [87] A. Seffah, M. Donyaee, R. B. Kline and H. K. Padda, "Usability measurement and metrics: A consolidated model", *Software Quality Control*, Vol. 14, No. 2, June 2006, pp. 159-178, DOI [10.1007/s11219-006-7600-8](https://doi.org/10.1007/s11219-006-7600-8)
- [88] The Encyclopedia of Human-Computer Interaction, 2nd Ed., Usability Evaluation, <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/usability-evaluation>
- [89] N. Bevan and M. Macleod, "Usability Measurement in Context", *Behaviour and Information Technology*, Vol. 13, No. 1-2, January 1994, pp. 132-145, DOI [10.1080/01449299408914592](https://doi.org/10.1080/01449299408914592)
- [90] A. Seffah and E. Metzker, "The obstacles and myths of usability and software engineering", *Communications of the ACM*, Vol. 47, No. 12, December 2004, pp. 71-76, DOI [10.1145/1035134.1035136](https://doi.org/10.1145/1035134.1035136)
- [91] M. Y. Ivory and M. A. Hearst, "The state of the art in automating usability evaluation of user interfaces", *ACM Computing Surveys*, Vol. 33, No. 4, December 2001, pp. 470-516, DOI [10.1145/503112.503114](https://doi.org/10.1145/503112.503114)

- [92] S. Rosenbaum, "Usability evaluations versus usability testing: when and why?", IEEE Transactions on Professional Communication, Vol. 32, No. 4, December 1989, pp. 210-216, DOI [10.1109/47.44533](https://doi.org/10.1109/47.44533)
- [93] D. G. Novick and T. Hollingsed, "Usability inspection methods after 15 years of research and practice", SIGDOC '07: 25th annual ACM international conference on Design of communication, El Paso, Texas (USA), October 22-24, 2007, pp. 249-255, DOI [10.1145/1297144.1297200](https://doi.org/10.1145/1297144.1297200)
- [94] 10 Usability Heuristics for User Interface Design, <https://www.nngroup.com/articles/ten-usability-heuristics/>
- [95] J. Nielsen, "Enhancing the explanatory power of usability heuristics", CHI '94: ACM Conference on Human Factors in Computer Systems, Boston, Massachusetts (USA), April, 1994, pp. 152-158, DOI [10.1145/191666.191729](https://doi.org/10.1145/191666.191729)
- [96] Usability Testing, <https://www.usability.gov/how-to-and-tools/methods/usability-testing.html>
- [97] K. L. Norman and E. Panizzi, "Levels of automation and user participation in usability testing", Interacting with Computers, Vol. 18, No. 2, March 2006, pp. 246-264, DOI [10.1016/j.intcom.2005.06.002](https://doi.org/10.1016/j.intcom.2005.06.002)
- [98] H. Aziz, "Comparison between Field Research and Controlled Laboratory Research", Archives of Clinical and Biomedical Research, Vol. 1, April 2017, pp. 101-104, DOI [10.26502/acbr.50170011](https://doi.org/10.26502/acbr.50170011)
- [99] S. Rosenbaum and L. Kantner, "Field Usability Testing: Method, Not Compromise", IEEE International Professional Communication Conference, Seattle, WA (USA), October 1-3, 2007, pp. 152-158, DOI [10.1109/IPCC.2007.4464060](https://doi.org/10.1109/IPCC.2007.4464060)
- [100] L. Kantner, D. H. Sova and S. Rosenbaum, "Alternative methods for field usability research", SIGDOC '03: ACM 21st Annual International Conference on Documentation, San Francisco, CA (USA), October 2003, pp. 68-72, DOI [10.1145/944868.944883](https://doi.org/10.1145/944868.944883)
- [101] A. Oztoprak and C. Erbug, "Field versus Laboratory Usability Testing: a First Comparison", <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.1359&rep=rep1&type=pdf>
- [102] C. Thomas and N. Bevan, "Usability Context Analysis: A Practical Guide", HUSAT, 1996, <https://core.ac.uk/reader/288385592>
- [103] Usability Evaluation Basics, <https://www.usability.gov/what-and-why/usability-evaluation.html>
- [104] A. Abran, A. Khelifi, W. Suryn and A. Seffah, "Usability Meanings and Interpretations in ISO Standards", Software Quality Control, Vol. 11, No. 4, November 2003, pp. 325-338, DOI [10.1023/A:1025869312943](https://doi.org/10.1023/A:1025869312943)
- [105] D. Gupta, A. K. Ahlawat and Kalpna Sagar, "Usability Prediction & Ranking of SDLC Models Using Fuzzy Hierarchical Usability Model", Open Engineering, Vol. 7, No. 1, January 2017, pp. 161-168, DOI [10.1515/eng-2017-0021](https://doi.org/10.1515/eng-2017-0021)
- [106] A. M. Lund, "Measuring Usability with the USE Questionnaire", Usability and User Experience Newsletter of the STC Usability SIG, Vol. 8, No. 2, January 2001, pp. 3-6
- [107] L. Longo, "Subjective Usability, Mental Workload Assessments and Their Impact on Objective Human Performance", INTERACT: IFIP Conference on Human-Computer Interaction, Mumbai (India), September 25-29, 2017, pp. 202-223, DOI [10.1007/978-3-319-67684-5_13](https://doi.org/10.1007/978-3-319-67684-5_13)
- [108] B. C. K. Choi and A. W. P. Pak, "A Catalog of Biases in Questionnaires", Preventing chronic disease, Vol. 2, No. 1, January 2005, pp. 1-13
- [109] S. R. Valdehita, E. Díaz Ramiro, J. M. García and J.M. Puente, "Evaluation of subjective mental workload: a comparison of SWAT, NASA-TLX, and Workload Profile Methods", Applied Psychology, Vol. 53, No. 1, January 2004, pp. 61-86
- [110] S. S. Potter and J. R. Bressler, "Subjective Workload Assessment Technique (SWAT): A User's Guide", 1989, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a215405.pdf>
- [111] System Usability Scale (SUS), <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>
- [112] A. Fruhling and S. Lee, "Assessing the Reliability, Validity and Adaptability of PSSUQ", 11th Americas Conference on Information Systems, Omaha, NE (USA), August 11-14,

- 2005, pp. 2394-2402
- [113] Questionnaire for User Interface Satisfaction (QUIS), <https://ext.eurocontrol.int/ehp/?q=node/1611>
 - [114] J. Kirakowski, "The software usability measurement inventory: background and usage" in the book "Usability Evaluation In Industry" edited by P. W. Jordan, B. Thomas, I. L. McClelland and B. Weerdmeester, 1996, pp. 169-176, DOI [10.1109/HICSS.2004.1265412](https://doi.org/10.1109/HICSS.2004.1265412)
 - [115] L. Herman, "Towards effective usability evaluation in Asia: cross-cultural differences", OZCHI '96: 6th Australian Conference on Computer-Human Interaction, Hamilton, New Zealand (New Zealand) , November 24-27, 1996, pp. 135-136, DOI [10.1109/OZCHI.1996.559999](https://doi.org/10.1109/OZCHI.1996.559999)
 - [116] K. Hornbaek, "Current practice in measuring usability: Challenges to usability studies and research", International Journal of Human-Computer Studies, Vol. 64, No. 2, February 2006, pp. 79-102, DOI [10.1016/j.ijhcs.2005.06.002](https://doi.org/10.1016/j.ijhcs.2005.06.002)
 - [117] T. Lin and W. Hu, "Do physiological data relate to traditional usability indexes?", OZCHI '05: 17th Australian Conference on Computer-Human Interaction, Canberra (Australia) , November 23-25, 2005, pp. 1-10, DOI [10.5555/1108368.1108405](https://doi.org/10.5555/1108368.1108405)
 - [118] V. do Amaral, L. A. Ferreira, P. T. Aquino and M. C. F. de Castro, "EEG signal classification in usability experiments", ISSNIP Biosignals and Biorobotics Conference, Rio de Janeiro (Brazil) , February 18-20, 2013, pp. 1-5, DOI [10.1109/BRC.2013.6487469](https://doi.org/10.1109/BRC.2013.6487469)
 - [119] R. L. Mandryk, M. S. Atkins and K. M. Inkpen, "A continuous and objective evaluation of emotional experience with interactive play environments", CHI '06: CHI 2006 Conference on Human Factors in Computing Systems, Montréal Québec (Canada) , April, 2006, pp. 1027-1036, DOI [10.1145/1124772.1124926](https://doi.org/10.1145/1124772.1124926)
 - [120] L. M. Hirshfield, E. T. Solovey, A. Girouard, J. Kebinger, R. J. K. Jacob, A. Sassaroli and S. Fantini, "Brain measurement for usability testing and adaptive interfaces: an example of uncovering syntactic workload with functional near infrared spectroscopy", CHI '09: CHI Conference on Human Factors in Computing Systems, Boston, MA (USA) , April, 2009, pp. 185-219, DOI [10.1145/1518701.1519035](https://doi.org/10.1145/1518701.1519035)
 - [121] R. McCraty and D. Tomasino, "Coherence-Building Techniques and Heart Rhythm Coherence Feedback: New Tools for Stress Reduction, Disease Prevention and Rehabilitation" in the book "Clinical Psychology and Heart Disease" edited by Springer, Milano, 2006, pp. 487-509, DOI [10.1007/978-88-470-0378-1_26](https://doi.org/10.1007/978-88-470-0378-1_26)
 - [122] K. Hercegf, "Heart Rate Variability Monitoring during Human-Computer Interaction", Acta Polytechnica Hungarica, Vol. 8, No. 5, 2011, pp. 205-224
 - [123] R. J. K. Jacob and K. S. Karn, "Commentary on Section 4 - Eye Tracking in Human-Computer Interaction and Usability Research: Ready to Deliver the Promises" in the book "The Mind's Eye" edited by J. Hyona, R. Radach and H. Deubel, 2003, pp. 573-605, DOI [10.1016/B978-044451020-4/50031-1](https://doi.org/10.1016/B978-044451020-4/50031-1)
 - [124] M. Mihajlov, B. J. Blazic and S. Josimovski, "Quantifying Usability and Security in Authentication", COMPSAC '11: 2011 IEEE 35th Annual Computer Software and Applications Conference, Munich, (Germany) , July 18-22, 2011, pp. 626-629, DOI [10.1109/COMP-SAC.2011.87](https://doi.org/10.1109/COMP-SAC.2011.87)
 - [125] J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", 33rd IEEE Symposium on Security and Privacy, San Francisco, CA (USA) , May 20-23, 2012, pp. 553-567, DOI [10.1109/SP.2012.44](https://doi.org/10.1109/SP.2012.44)
 - [126] V. Zimmermann and N. Gerber, "The password is dead, long live the password - A laboratory study on user perceptions of authentication schemes", International Journal of Human-Computer Studies, Vol. 133, January 2020, pp. 26-44, DOI [10.1016/j.ijhcs.2019.08.006](https://doi.org/10.1016/j.ijhcs.2019.08.006)
 - [127] N. Kumar, "Password in practice: An usability survey", Journal of Global Research in Computer Science, Vol. 2, No. 5, May 2011, pp. 107-112
 - [128] M. Belk, A. Pamboris, C. Fidas, C. Katsini, N. Avouris and G. Samaras, "Sweet-spotting security and usability for intelligent graphical authentication mechanisms", WI '17: International Conference on Web Intelligence 2017, Leipzig (Germany), August 20-23, 2017, pp. 252-259, DOI [10.1145/3106426.3106488](https://doi.org/10.1145/3106426.3106488)

- [129] E. E. Schultz, R. W. Proctor, M-C. Lien and G. Salvendy, "Usability and Security An Appraisal of Usability Issues in Information Security Methods", *Computers & Security*, Vol. 20, No. 7, October 2001, pp. 620-634, DOI [10.1016/S0167-4048\(01\)00712-X](https://doi.org/10.1016/S0167-4048(01)00712-X)
- [130] C. S. Weir, G. Douglas, T. Richardson and M. Jack, "Usable security: User preferences for authentication methods in eBanking and the effects of experience", *Interacting with Computers*, Vol. 22, No. 3, May 2010, pp. 153-164, DOI [10.1016/j.intcom.2009.10.001](https://doi.org/10.1016/j.intcom.2009.10.001)
- [131] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny and L. J. Camp, "A qualitative study on usability and acceptability of Yubico security key", *STAST2017: 7th International Workshop on Socio-Technical Aspects in Security and Trust*, Orlando, FL (USA), December, 2017, pp. 29-39, DOI [10.1145/3167996.3167997](https://doi.org/10.1145/3167996.3167997)
- [132] V. Matyas and Z. Ríha, "Biometric Authentication - Security and Usability", *IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security*, Portoroz (Slovenia), September 26-27, 2002, pp. 227-239, DOI [10.1007/978-0-387-35612-9_17](https://doi.org/10.1007/978-0-387-35612-9_17)
- [133] L. M. Mayron, Y. Hausawi and G. S. Bahr, "Secure, Usable Biometric Authentication Systems", *UAHCI 2013: International Conference on Universal Access in Human-Computer Interaction*, Las Vegas, NV (USA), July 21-26, 2013, pp. 195-204, DOI [10.1007/978-3-642-39188-0_21](https://doi.org/10.1007/978-3-642-39188-0_21)
- [134] A. Felstead and G. Henseke, "Assessing the growth of remote working and its consequences for effort, well-being and work-life balance", *New Technology, Work and Employment*, Vol. 32, No. 3, November 2017, pp. 195-212, DOI [10.1111/ntwe.12097](https://doi.org/10.1111/ntwe.12097)
- [135] Remote Access VPN: Secure Your Access Point in 2020, <https://www.purevpn.com/blog/secure-remote-access-vpn-solution/>
- [136] OIDC Auth Method, <https://learn.hashicorp.com/vault/identity-access-management/oidc-auth>
- [137] UML Diagrams for ATM Machine, <http://www.programsformca.com/2012/03/uml-diagrams-for-atm-machine.html>
- [138] V. Moncur and G. Leplatre, "Pictures at the ATM: exploring the usability of multiple graphical passwords", *CHI '07: CHI Conference on Human Factors in Computing Systems*, San Jose, CA (USA), April, 2007, pp. 887-894, DOI [10.1145/1240624.1240758](https://doi.org/10.1145/1240624.1240758)
- [139] Managing Knowledge-Based Authentication, https://docs.oracle.com/cd/E21043_01/doc.1111/e14568/kba.htm#CFHFIHDJ
- [140] Cryptanalysis of a Cognitive Authentication Scheme, <https://www.slideserve.com/haile/cryptanalysis-of-a-cognitive-authentication-scheme>
- [141] European Central Bank, <https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.html>
- [142] ATM logic attacks: scenarios, 2018, <https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/>
- [143] Terminal Fraud Definitions, <https://www.association-secure-transactions.eu/industry-information/terminal-fraud-definitions/>
- [144] FBI warning: Cyberthieves mining social media for personal data to hack accounts, <https://www.post-gazette.com/business/tech-news/2020/04/24/FBI-warns-sharing-personal-information-could-lead-to-password-problems-hackers/stories/202004240098#:~:text=FBI%20warning%3A%20Cyberthieves%20mining%20social%20media%20for%20personal%20data%20to%20hack%20accounts,-Torsten%20Ove&text=With%20millions%20of%20Americans%20stuck,access%20to%20password%2Dprotected%20accounts.>
- [145] 4 Big Problems with Knowledge Based Authentication, <https://nudatasecurity.com/resources/blog/risk-based-authentication/4-big-problems-with-knowledge-based-authentication/>
- [146] A new low for knowledge-based authentication?, <https://www.javelinstrategy.com/blog/new-low-knowledge-based-authentication>
- [147] S. Gupta, S. Shashank, P. Sabbu, S. Varma and S. Gangashetty, "Passblot: A Highly Scalable Graphical One Time Password System", *International Journal of Network Security & Its Applications*, Vol. 2, No. 2, March 2012, pp. 201-216, DOI [10.5121/ijnsa.2012.4215](https://doi.org/10.5121/ijnsa.2012.4215)

- [148] Your Android unlock pattern, <https://boingboing.net/2015/08/20/your-android-unlock-pattern-su.html>
- [149] Grid Authentication, <https://ru.sentinelcloud.com/multi-factor-authentication/authenticators/grid-authentication/>
- [150] M. K. Mat Kiah, and Y. Por, "Shoulder Surfing Resistance Using PENUP Event And Neighboring Connectivity Manipulation", Malaysian Journal of Computer Science, Vol. 23, No. 2, September 2010, pp. 121-140, DOI [10.22452/mjcs.vol23no2.5](https://doi.org/10.22452/mjcs.vol23no2.5)
- [151] M. Masrom, F. Towhidi and A. Habibi Lashkari, "Pure and cued recall-based graphical user authentication", AICT 2009: International Conference on Application of Information and Communication Technologies, Baku (Azerbaijan), October 14-16, 2009, pp. 1-6, DOI [10.1109/ICAICT.2009.5372534](https://doi.org/10.1109/ICAICT.2009.5372534)
- [152] A. Habibi Lashkari, A. Gani, L. Ghasemi Sabet and S. Farmand, "A New Algorithm on Graphical User Authentication (GUA) Based on Multi-line Grids", Scientific Research and Essays, Vol. 5, No. 24, December 2010, pp. 3865-3875
- [153] S. Chiasson, A. Forget, R. Biddle and P. C. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click-Points", BCS-HCI '08: 22nd British HCI Group Annual Conference on People and Computers, Liverpool (UK), September 1-5, 2008, pp. 121-130, DOI [10.5555/1531514.1531531](https://doi.org/10.5555/1531514.1531531)
- [154] A. R. Karia and A. B. Patankar, "Image Based Authentication Using Persuasive Cued Click Points", Int. Journal of Engineering Research and Applications, Vol. 4, No. 5, May 2014, pp. 179-185
- [155] Passfaces SDK Overview, <http://www.realuser.com/enterprise/products/Brochures/Passfaces%20SDK.pdf>
- [156] J. Nielsen and J. Levy, "Measuring usability: preference vs. performance", Communications of the ACM, Vol. 37, No. 4, April 1994, pp. 66-75, DOI [10.1145/175276.175282](https://doi.org/10.1145/175276.175282)
- [157] The dangers of self-report, <https://www.sciencebrainwaves.com/the-dangers-of-self-report/>
- [158] Discount Usability for the Web, <https://www.nngroup.com/articles/web-discount-usability/>
- [159] NIST Special Publication 800-63B Digital Identity Guidelines, <https://pages.nist.gov/800-63-3/sp800-63b.html#sec3>
- [160] L. N. Tiller, C. A. Angelini, S. C. Leibner and J. D. Still, "Explore-a-Nation: Combining Graphical and Alphanumeric Authentication", HCII 2019: International Conference on Human-Computer Interaction, Orlando, FL (USA), July 26-31, 2019, pp. 81-95, DOI [10.1007/978-3-030-22351-9_6](https://doi.org/10.1007/978-3-030-22351-9_6)
- [161] OTP - One Time Password, <https://www.partnerdata.it/prodotti/identificazione/one-time-pw/>
- [162] Deepnet security, <https://deepnetsecurity.com/authenticators/one-time-password/safeid/>
- [163] Monclick - Smartcard reader, <https://www.monclick.it/prodotti/13/LSC/digicom/8E4479.htm#img2>
- [164] ACompany - Token OTP, https://www.firmaemarca.com/isms_soho_it/otp-usb.html
- [165] Printable Smooth RFID Chip Blank Card 13.56 MHz Ntag215 NFC Card, https://www.alibaba.com/product-detail/Printable-Smooth-RFID-Chip-Blank-Card_60597341360.html
- [166] Two Factor SMS Authentication, <http://www.360globalsolutions.com/two-factor-sms-authentication.html>
- [167] M2SYS - How fingerprint scanner works, <https://www.m2sys.com/blog/important-biometric-terms-to-know/fingerprint-vs-vascular-biometrics-what-are-the-differences/attachment/how-fingerprint-scanner-works/>
- [168] Face Id: Deep learning for face recognition, <https://medium.com/@fenjiro/face-id-deep-learning-for-face-recognition-324b50d916d1>
- [169] How the iris scanner on the Note 7 works, <https://www.androidpit.com/how-the-iris-scanner-on-the-note-7-works>

- [170] Biometric System Laboratory, DISI - University of Bologna, <https://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=222&pathSubj=222&Req=&>
- [171] E. Lee, H. Yeh, H-S. Yang, S. Moon and O. Choi, "A Secure NFC-Based Mobile Printing Service Using Recognition Robot", International Journal of Distributed Sensor Networks, Vol. 2015, September 2015, pp. 1-7, DOI [10.1155/2015/564506](https://doi.org/10.1155/2015/564506)
- [172] ADI collaboration brings ECG biometric authentication to the car, <https://www.eenewseurope.com/news/adi-collaboration-brings-ecg-biometric-authentication-car-0>
- [173] Subtleties of Eyetracking Heat Maps and Gaze Plots, <https://medium.com/@TheRealTang/subtleties-of-eyetracking-heat-maps-and-gaze-plots-a7ba4207f20f>