Feasibility Study of a Multimodal Biometric Authentication Solution Based on Pointer Dynamics and Skin Conductivity

Vítor J. Sá[1,3], Sérgio T. Magalhães[1,3], Henrique D. Santos[2,3]

[1] Faculdade de Ciências Sociais, Universidade Católica Portuguesa, Braga, Portugal
{vitor.sa, stmagalhaes}@braga.ucp.pt
[2] Departamento de Sistemas de Informação, Universidade do Minho, Guimarães, Portugal
hsantos@dsi.uminho.pt
[3] Centro Algoritmi, Universidade do Minho, Guimarães, Portugal

Abstract. Due to the constant need to improve authentication systems, since they are constantly emerging new forms of intrusion, based on the current state of knowledge, we intend to study the acceptance of a recognition system based on the combination of two non-physical methods of biometric authentication: pointer dynamics and skin conductivity. With this combination, firstly, it is improved what each can offer individually and, secondly, the problem of replicability present in physical biometric is minimized. We conducted a survey with a representative sample of the Portuguese population, whose construction method and obtained results are presented in this article. We also present an introductory explanation of the involved technologies.

Keywords: biometrics; graphical authentication; pointer dynamics; skin conductivity; multimodal; acceptance.

1 Introduction

This article falls within the field of recognition of users, given the way the interaction with the computer is performed. This induces a crossing of distinct areas, but not as divergent as might appear at first sight, such as human-computer interaction, electrophysiology and computer graphics.

The recognition of users consists in accurately determine the identity of those who wish to access certain services/systems. The mechanism for this is always based in the principle of establishing a link between an individual and a digital identity. Recognition can be divided into two main categories, identification and authentication, as the intention is, respectively, to determine or to confirm the identity of the user (Boulgouris, Plataniotis & Micheli-Tzanakou, 2010).

The passwords have been the most common form of authentication, but also one of the major forms of hacking; either by online password guessing attacks or by offline dictionary attacks (Gabi and Al-Nemrat, 2012). The issue of passwords is paradoxical, and his ill-treatment is a major cause of intrusion in an information

system. On the one hand, following a few rules, the passwords must be complex, if possible randomly generated, different from system to system, and have a reasonable number of characters, on the other hand, this makes them difficult to remember (Yan, Blackwell, Anderson, & Grant, 2004), leading to the need to store them in places that are sometimes unsafe. To overcome these difficulties many choose to do the opposite: the use of only one password for all systems, that is reduced in size and easy to remember (Lach, 2010), simultaneously reducing security.

The only way to overcome the transmissibility problem of the passwords is through the recognition of characteristics of individuals, something intrinsic to the person and which distinguishes him in a unique and intransmissible way, i.e. through the procedures currently in research and improvements known as biometrics.

But biometrics is not foolproof because it can be replicated. Today there are several fraudulent ways to replicate a biometric characteristic. This raises new challenges in this field. They are then required new effective and efficient authentication schemes, in which behavioural and multimodal biometrics play an important role, as well as cognitive biometrics, which uses biological signals representative of the mental and emotional states for the authentication of users.

Thus, we have identified the following problems: replicability is possible even with the common biometric technology; some types of applications have the requirement of continuous authentication; there is a constant need to improve the accuracy of the systems (information systems with more users imply a need to lower error rates); there is a constant need (inherent to the existence of a business) to lower the cost; there is a need to keep the mobility of some systems, with restrictions on the type of hardware (dimension, energy, etc.) and on the use conditions (light, noise, etc.).

Recent work in non-conventional biometrics, particularly in the conductivity of the skin seems to indicate that this technology has potential (with or without activation of the knowledge component). The current size of the conductivity sensors enables its integration into mobile devices. There is also work done and consolidated in gesture dynamics.

However, it would be useless to develop a technology with innovative features to solve certain type of authentication problems if, after its implementation, this same technology has not acceptance by people. Therefore, we want to know the adoption rate, in Portugal (mainland), of a technology with features such as those we talking about. Find answers to this question is the main objective of this work. To this end, based on the Technology Acceptance Model (TAM), we sought to develop a system of structural equations that allow predicting the level of adoption of such technology.

In sections 2 we present the topic of graphical authentication with the goal to, in section 3, talk about its junction with a biometric layer to obtain the pointer dynamics behavioural biometrics. Still in section 3 we explain the possibility to use galvanic skin response for recognition of individuals, in a scenario of multimodal biometric authentication. In section 4 we present the acceptance study that was followed, including the adopted model, the inquiry tool and the analysis of results. Finally, in section 5, we draw conclusions and outline future work.

2 Graphical Authentication

A simple way to overcome the password paradox is to find a process of increasing the complexity of the secret without embarrass memorization. This can be achieved by taking advantage of the fact that human beings have greater ability to recognize visual information than to recognize sequences of characters without semantics (Nickerson, 1965; Shepard, 1967; Standing, 1973).

The graphical authentication consists in matching a set of images, or a set of points of an image, to the identity of an individual. The user selects a set of graphic elements, and that sequence of elements previously referenced constitute the authentication secret. These systems can be easily adapted to generate traditional passwords, more complex and easier to remember. The concept of graphical password was patented in 1995 by Blonder (Blonder, 1996).

Due to the continuing proliferation of mobile computing, graphical authentication forms are increasingly important. The authentication techniques based on knowledge are the most widely used and include both text-based passwords as image-based passwords. Suo, Zhu, & Owen, 2006, proposed a taxonomy that divided the passwords as being based on recognition ("recognition based") or on memory ("recall-based") and within these classes as being more related to visualization or to interaction.

The memory-based techniques can be subdivide into two types: reproduce a drawing (Draw-a-secret) or repeat a selection (Passlogix and PassPoint). The Manual Signature belongs to the first type because, in its essence, it consists in the reproduction of a drawing that the user must repeat to be authenticated. The Draw-a-secret authentication scheme was initially thought to be used on PDAs (Personal Digital Assistants). This technique consists in the reproduction of a design previously generated by the user in a grid. This design is associated with a sequence of coordinate pairs. The authentication consists in reproduce the design, that is, go through the grid according to the same coordinates and in the same order.

This technique has as advantages the ability to generate long codes and the difficulty of imitation of the original design. Although it can also be used in normal screens, in addition to handheld computers, it is not recommended for use in public places.

The Passlogix is based on the idea of Blonder. The user must click several items in the image, in the correct sequence, in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by the mouse or not (Paulson, 2002).

The PassPoint technique, proposed by Wiedenbeck et al. (Wiedenbeck, Waters, Birget, Brodskiy & Memon, 2005), extends the Blonder's idea eliminating the pre-defined borders and allowing the use of arbitrary images. As a result, the user can click anywhere on the image (unlike some pre-defined areas) to create a password. The tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance space of their chosen pixels and also in the correct sequence.

3 Non-conventional Biometrics

3.1 Pointer Dynamics

Pointer dynamics is a biometric graphical authentication that is obtained by adding behavioural biometric techniques, such as those used in keystroke dynamics, during the graphical interaction. Proposed by Magalhães in 2008 (Fig. 1), this experimental concept aims to set the user pattern when using a pointing device (mouse, stylus, touch pad, etc.) to authenticate in a graphical authentication system. In each authentication attempt, the access is permitted if and only if the pattern existing in how the graphic secret was introduced is similar to the pattern previously stored of the rightful user (Magalhães, 2008).

The authentication phase consists of, for each two selected points, collect the elapsed time (called proposed time, PT, because is being proposed as a legitimate time) and compare it with the corresponding value stored in the registration phase, using a checking criterion defined by the formula shown bellow, where α is a parameterizable variable (SD is the standard deviation).

$$min(average; median) * (1 - \alpha - \frac{\text{SD}}{average}) \leq PT \leq max(average; median) * (1 + \alpha + \frac{\text{SD}}{average})$$

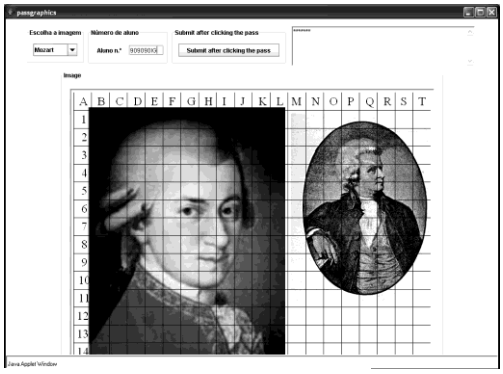

Fig. 1. Example of a passgraph authentication window (source: Magalhães, 2008)

3.2 Galvanic Skin Response

The galvanic skin response (or the skin conductivity, or the psychogalvanic reflex) has been considered a cognitive biometrics. What makes a particular biometric be classified as cognitive is the fact that it serve to recognize a person after the reaction of a stimulus, through the collection of biological signals using electrocardiograms (ECG), electroencephalograms (ECG) and, in this case, electrodermal responses (EDR). These biological signals can be acquired in various circumstances during a human-machine interaction. Each of these signals provides a range of information that

can be extracted easily, with the goal of obtaining an authentication. The EDR measure the electrical conductance of the skin, which varies with its humidity level, caused by a specific sweat glands (Mandryk & Atkins, 2007). The sweat glands are controlled by the nervous system; hence it is used as an indication of psychological or physiological excitation. An EDR is highly sensitive to emotions in some people, such as feelings of fear, anger, and startle response, among others, which can produce varied responses in terms of skin conductance. The resistance of gland in a hand palm varies even though the sweat may not reach the surface of the skin yet (Stern, Ray & Quigley, 2001). These reactions have been used as part of the polygraph or lie detector (Reid & Inbau, 1977).

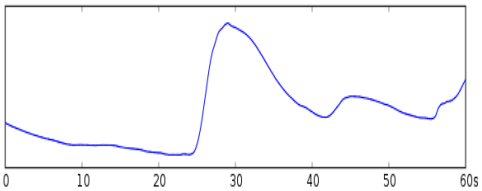

Fig. 2. EDR signal to a sample of 60s

These signals can be measured using the same technology as ECG and EEG. Figure 2 shows a typical signal of an EDR measuring the electrical conductivity between two points.

Thus, once an EDR provides information about the emotional states of an individual, such data may be used for user authentication, although at present there is little published information that proves the use of EDR as a biometric technique. However, because of determining whether an individual is nervous during authentication, for example, justify the use of this measure, in combination with other biometric techniques, so as to ensure safe access. In addition, electrodes for capturing an EDR may be positioned more or less anywhere in the body, since the signal is not affected by muscle activity. Likewise, the EDR can be more individualized that the other two signal capture methods because, in theory, there is a genetic factor associated with individual characteristics of the ECG/EEG (Revett, Deravi and Sirlantzis, 2010).

3.3 Multimodal Biometrics

Multimodal biometrics refers to the use of more than one source of information for biometric recognition (Ross and Jain, 2004; Faria, Sá and Magalhães, 2011).

The problem with combining two or more identity tests seems paradoxical. If, on one hand, it seems clear that more information is better than less information, on the other hand, by combining a strong test with a weaker test the efficiency of the system is between the two tests, namely worse than stronger and better than the weakest (Daugman, 2011). From this point of view it is concluded that we should not match a strong biometrics with a weak biometrics.

In other situations unimodal strategies are inadequate taking into account the cost of implementation, which may be high for a high degree of accuracy, compared with a multimodal solution that may have a lower precision considering the biometrics alone but with a higher quality when combined, as well as a lower implementation cost (Bhattacharya, Srivastava, Rajakoti, & Kumar, 2011).

It can be found very interesting multimodal solutions since the system is correctly configured, that is, provided that the thresholds values of the biometrics are properly combined to assist each other, instead of having two independent security mechanisms.

A multimodal system can operate in serial mode, parallel mode and hierarchical mode. In serial mode the number of possible identities will reduce from modality to modality, and the decision may be taken before all the catches, in parallel mode information from various modalities are used simultaneously, and in hierarchical mode the different recognitions are classified in a trees structure (Ross & Jain, 2004).
In the context of implementation, it is possible to distinguish two classes of multimodal systems - one in which the signal integration occurs at the level of its characteristics (early fusion) and another where integration occurs at a semantic level (late fusion). (Sá, Malerczyk & Schnaider, 2001).

4 Acceptance Study

4.1 Model

The acceptance of technology is a matter of utmost importance in research in information systems research. It is essential to understand whether a given population will accept or reject a technology, which relies on objective and subjective factors and on the context in which it occurs. Researchers have studied this topic with a high incidence since the mid-90s, and it's possible to identify several theories in the literature to predict the impact of technology on human behaviour. The three theories of technology acceptance that stand out are: Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1975), Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw, 1989) and Theory of Planned Behavior (TPB) (Ajzen, 1991).

In this work we used the Technology Acceptance Model (TAM) to be the most known and used in the area of information systems, not the original from Davis et al., 1989, but the one from Malhotra & Galleta, 1999, which includes the Psychological Link from Kelman, 1958, and the questionnaire from O'Reilly et al., 1991, that, meanwhile, was adapted for information systems. TAM seeks to provide a basis for assessing the impact of external variables (characteristics of the system, development process, etc.) in beliefs and attitudes. The relevant beliefs are Perceived Usefulness and Perceived Ease of Use.

As with any new technology, acceptance by the user of new software/hardware system is often difficult to assess and are often non-existent policies to introduce and ensure the correct and appropriate use of such technologies. In many situations the lack of adoption of technology has nothing to do with the technology itself, but rather

with the lack of preparedness, or elucidation of users on its functioning (Borges, Sá, Magalhães, & Santos, 2012).

Security technologies have a wide applicability to different organizational contexts that may present adoption considerations unusual and varied. Biometry, in particular, presents even greater adoption concerns because they add invasion levels for the user that are obvious. The work of James et al., 2006, consisted of the adaptation of the TAM for this type of technology, for which were included mechanisms for perception of privacy need, for perception of security need and perception of physical invasion of the biometric devices as factors influencing the intention to use (James, Pirim, Boswell, Reithel, & Barkhi, 2006). In our case, the prototype we set ourselves, although it fits in cognitive biometrics, with all that may suggest invasive due to the necessary devices for signal reception, in fact it is not, since the idea is to use the back side of a mobile device and, justifiably, we do not need the TAM extension.

4.2 Survey Construction

O'Reilly et al. in 1991 developed a model of questionnaire with 12 items (O'Reilly, Chatman, & Caldwell, 1991), later adapted by Malhotra & Galletta for information systems (Malhotra & Galletta, 1999). In this work we developed a questionnaire with the same type of questions, thus avoiding the need for validation.

The aim was not to evaluate the current level of adoption of a technology, but the potential level of adoption. Therefore the respondent was confronted with a hypothetical situation to verify, in case of adoption, its acceptance. Given this constraint, it was necessary to make some adjustments to the questionnaire, putting the verb tenses in the conditional (e.g. instead of "it's easy for you to introduce a passgraph?" we have "would be easy for you to introduce a passgraph?").

We used a likert scale from 1 to 7. After two filter questions, to find out if a person has some connection with technology and if he has any touch screen device, the questions are divided in two groups. The first one is the Perceived Usefulness and Perceived Ease of Use, which include questions like: "it would be easy for you, enter a sequence secretly via a touch screen, remaining two fingers in two fixed positions on the back of the device" or "considers that the use of biometrics that measure the emotional state (cognitive biometrics) make your tasks safer". The second one is the Psychological Link that includes questions like: "feel proud to use cognitive biometrics".

4.3 Data Analysis

The survey covers the whole country (mainland), which were made about 1000 phone calls, in which only 250 people showed up ready to respond, but not all decided to answer to all questions. The statistical treatment of the data was made with the STATA software.

Mean estimation Number of obs = 207

	Mean	Std. Err.	[95% Conf.	Interval]
utilidade	4.985507	.0636868	4.859946	5.111069
LigPsi2	5.096618	.0494014	4.999221	5.194015

Fig. 3. Usefulness and psychological link

The main deductions from the collected data are that there is a favourable perception of usefulness (> 4) and that there is psychological link (> 4) (Fig. 3).

. proportion Seria_fcil if Seria_fcil<8

Proportion estimation Number of obs = 207

	Proportion	Std. Err.	[95% Conf.	Interval]
Seria_fcil				
1	.0096618	.0068153	-.0037749	.0230986
2	.0096618	.0068153	-.0037749	.0230986
3	.0241546	.0106969	.0030652	.045244
4	.0531401	.0156286	.0223276	.0839526
5	.1884058	.0272448	.1346915	.2421201
6	.2995169	.0319136	.2365977	.3624361
7	.4154589	.0343351	.3477657	.4831521

Fig. 4. Easy of use by qualifications

. kwallis utilidade if Seria_fcil<8, by(Habilitacoes)

Kruskal-Wallis equality-of-populations rank test

Habilit~s	Obs	Rank Sum
1º Ciclo	1	33.00
2º Ciclo	5	418.50
3º Ciclo	36	2328.00
Ens. Sec.	85	8239.50
Ens. Sup.	79	10302.00

chi-squared = 34.352 with 4 d.f.
probability = 0.0001

chi-squared with ties = 38.923 with 4 d.f.
probability = 0.0001

Fig. 5. Usefulness by qualifications

We only considered the questionnaires that were completed in the evaluation component of Ease of Use and Perception of Usefulness, and it was found that between 58% and 84% say it would be very easy (> = 6) (Fig. 4). The Kruskal-Wallis test shows that there are differences depending on the qualifications on the Perception of Usefulness, the more qualifications, greater Perception of Usefulness (Fig. 5).

. kwallis utilidade if Seria_fcil<8, by(Sexo)

Kruskal-Wallis equality-of-populations rank test

Sexo	Obs	Rank Sum
Feminino	115	11782.50
Masculino	92	9745.50

chi-squared = 0.172 with 1 d.f.
probability = 0.6785

chi-squared with ties = 0.194 with 1 d.f.
probability = 0.6593

. kwallis utilidade if Seria_fcil<8, by(possui)

Kruskal-Wallis equality-of-populations rank test

possui	Obs	Rank Sum
Não	85	7581.00
Sim	122	13947.00

chi-squared = 8.818 with 1 d.f.
probability = 0.0030

chi-squared with ties = 9.973 with 1 d.f.
probability = 0.0016

Fig. 6. Kruskal-Wallis for Usefulness by sex and by possession

```
. ttest utilidade if Seria_fcil<8, by(possui)

Two-sample t test with equal variances
```

Group	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
Não	85	4.752941	.1096287	1.010727	4.534932	4.97095
Sim	122	5.147541	.0733137	.8097763	5.002397	5.292685
combined	207	4.985507	.0636868	.916294	4.859946	5.111069
diff		-.3945998	.1268137		-.6446261	-.1445735

```
    diff = mean(Não) - mean(Sim)                                  t =  -3.1117
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.0011         Pr(|T| > |t|) = 0.0021          Pr(T > t) = 0.9989
```

Fig. 7. t-Student for Usefulness by possession

```
. ttest utilidade if Seria_fcil<8, by(Sexo)

Two-sample t test with equal variances
```

Group	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
Feminino	115	4.965217	.0948164	1.016793	4.777387	5.153048
Masculin	92	5.01087	.0810446	.777352	4.849885	5.171855
combined	207	4.985507	.0636868	.916294	4.859946	5.111069
diff		-.0456522	.1284399		-.2988848	.2075805

```
    diff = mean(Feminino) - mean(Masculin)                        t =  -0.3554
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.3613         Pr(|T| > |t|) = 0.7226          Pr(T > t) = 0.6387
```

Fig. 8. t-Student for Usefulness by sex

Owning a device with touchscreen influences positively the Perceived Usefulness, which was confirmed both by the Kruskal-Wallis test and the t-Student. There is no evidence that gender influences the perceived usefulness (Fig. 6, Fig. 7 and Fig. 8).

```
. ttest LigPsi2 if Seria_fcil<8, by(Sexo)

Two-sample t test with equal variances
```

Group	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
Feminino	115	5.156522	.0683145	.732591	5.021191	5.291852
Masculin	92	5.021739	.0707922	.6790145	4.881119	5.162359
combined	207	5.096618	.0494014	.710762	4.999221	5.194015
diff		.1347826	.099215		-.0608299	.3303952

```
    diff = mean(Feminino) - mean(Masculin)                        t =   1.3585
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.9121         Pr(|T| > |t|) = 0.1758          Pr(T > t) = 0.0879
```

Fig. 9. t-Student for Psychological Link by sex

```
. ttest LigPsi2 if Seria_fcil<8, by(possui)

Two-sample t test with equal variances
```

Group	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
Não	85	5.070588	.0781226	.7202552	4.915233	5.225944
Sim	122	5.114754	.063962	.7064838	4.988124	5.241384
combined	207	5.096618	.0494014	.710762	4.999221	5.194015
diff		-.0441659	.1006173		-.2425433	.1542116

```
    diff = mean(Não) - mean(Sim)                                  t =  -0.4389
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.3306         Pr(|T| > |t|) = 0.6612          Pr(T > t) = 0.6694
```

Fig. 10. t-Student for Psychological Link by possession

From Figures 9 and 10 we can conclude that both the gender and the fact of owning a touch screen device does not influence the Psychological Link.

```
. tabulate utilidade EnsinoSuperior
```

utilidade	EnsinoSuperior Não	Sim	Total
2	1	0	1
3	9	0	9
4	41	6	47
5	54	39	93
6	21	28	49
7	2	6	8
Total	128	79	207

```
. tabulate LigPsi2 EnsinoSuperior
```

LigPsi2	EnsinoSuperior Não	Sim	Total
3	0	2	2
4	27	6	33
5	75	44	119
6	22	27	49
7	4	0	4
Total	128	79	207

Fig. 11. Usefulness and Psychological Link for individuals with higher education

```
. ttest utilidade if Seria_fcil<8, by(EnsinoSuperior)

Two-sample t test with equal variances

   Group |     Obs        Mean    Std. Err.   Std. Dev.   [95% Conf. Interval]
---------+--------------------------------------------------------------------
     Não |     128    4.710938    .0801023    .9062542    4.552429    4.869446
     Sim |      79     5.43038    .0838918    .7456462    5.263364    5.597395
---------+--------------------------------------------------------------------
combined |     207    4.985507    .0636868     .916294    4.859946    5.111069
---------+--------------------------------------------------------------------
    diff |           -.7194422    .1214335               -.9588609   -.4800236
------------------------------------------------------------------------------
    diff = mean(Não) - mean(Sim)                                  t =  -5.9246
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.0000         Pr(|T| > |t|) = 0.0000          Pr(T > t) = 1.0000
```

Fig. 12. t-Student for Usefulness by higher education

```
. ttest LigPsi2 if Seria_fcil<8, by(EnsinoSuperior)

Two-sample t test with equal variances

   Group |     Obs        Mean    Std. Err.   Std. Dev.   [95% Conf. Interval]
---------+--------------------------------------------------------------------
     Não |     128    5.023438    .0631997    .7150226    4.898377    5.148498
     Sim |      79     5.21519    .0778461    .6919109     5.06021    5.370169
---------+--------------------------------------------------------------------
combined |     207    5.096618    .0494014     .710762    4.999221    5.194015
---------+--------------------------------------------------------------------
    diff |           -.1917524    .1010571               -.390997    .0074922
------------------------------------------------------------------------------
    diff = mean(Não) - mean(Sim)                                  t =  -1.8975
Ho: diff = 0                                     degrees of freedom =      205

    Ha: diff < 0                 Ha: diff != 0                 Ha: diff > 0
 Pr(T < t) = 0.0296         Pr(|T| > |t|) = 0.0592          Pr(T > t) = 0.9704
```

Fig. 13. t-Student for Psychological Link by higher education

From Figures 11, 12 and 13 we can conclude that higher education possession affects positively the Perception of Usefulness but does not affect the Psychological Link.

5 Conclusion and future word

Although this type of technology is generally well accepted by people, there could be some fear when we tell the user we are measuring the skin conductivity. But only 25% presented that fear. If this process is transparent we think that even this problem disappears. The same happens with the current touch screens, with capacitive sensing technology (based on capacitive coupling), which takes human body capacitance as input; capacitive sensors detect anything that is conductive or has a dielectric difference from that of air.

The mobile phones of today are handheld computers that allow access to several other computers, or even computing centers that control the most diverse systems. It

is very easy for a stranger to seize someone's smartphone, and so it is very important to develop rigorous authentication techniques.

Direct use of the fingers as a form of interaction with touch screens devices has been asserting itself as a natural and effective means of communication. This mode of use, combined with the fact that the device has to be handled with other hand (in the most common situations) led us to the conception of the idea that we have been talking. In the authentication phase, either static, performed only at the beginning to allow access to the device, whether continuous, during use, to confirm the identity of the user, it becomes easy to imagine the design of a system of this type. We refer to the back side of the device, since for the front side there are not yet a technological solution to make a touch screen serves both for haptics and for detection of skin conductivity signs. This work has shown that is acceptable by users to do so.

Acknowledgments

This work was partially funded by FEDER Funds through the Operational Programme for Competitiveness Factors - COMPETE and National Funds through FCT - Foundation for Science and Technology under the Project: FCOMP-01-0124-FEDER-022674.

References

1. Ajzen, I., Fishbein, M. (1975) Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley
2. Bhattacharya, P., Srivastava, P. R., Rajakoti, A., & Kumar, V. V. (2011) An integrated authentication framework based on multi-tier biometrics. International Journal of Biometrics, 3(1), 13–39
3. Blonder, G.E. (1996) Graphical Password. Obtained from http://www.google.com/patents/US5559961
4. Borges, D., Sá, V.J., Magalhães, S.T., & Santos, H. (2012) Study of the Perception on the Biometric Technology by the Portuguese Citizens. In Global Security, Safety and Sustainability & e-Democracy (pp. 280-287). Springer Berlin Heidelberg
5. Boulgouris, N.V., Plataniotis, K.N. Micheli-Tzanakou, E. (2010) Biometrics: Theory, Methods, and Applications. Wiley-IEEE
6. Daugman, J. (2011). Combining Multiple Biometrics. Obtained in May 19th, from http://www.cl.cam.ac.uk/~jgd1000/combine/
7. Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science. 35. pp. 982-1003
8. Faria, L., Sá, V.J., Magalhaes, S.T. (2011) Multimodal cognitive biometrics. In 6th Iberian Conference on Information Systems and Technologies (CISTI), (pp. 1-6). IEEE
9. Gabi, D., Al-Nemrat, A. (2012) Password Guessing Attacks: Analysis and Discovery of Evidence in Computer Forensic Investigation. In: Weir, G. R., & Al-Nemrat, A. (Eds.), Issues in Cybercrime, Security and Digital Forensics, 53-72, University of Strathclyde Pub.

10. James, T., Pirim, T., Boswell, K., Reithel, B., Barkhi, R. (2006) Determining the intention to use biometric devices: An application and extension of the technology acceptance model. Journal of Organizational and End User Computing (JOEUC), 18(3), 1-24
11. Kelman, H.C. (1958) Compliance, Identification, and Internalization: Three Processes of Attitude Change? Journal of Conflict Resolution, 2, 51-60
12. Lach, J. (2010) Using Mobile Devices for User Authentication. In Kwiecień, A., Gaj, P., Stera, P. (eds.) Computer Networks, 79, 263-268. Springer: Berlin, Heidelberg
13. Magalhães, P.S. (2008) Estudo de viabilidade da utilização de tecnologias biométricas comportamentais na autenticação do cidadão perante os serviços electrónicos do Estado (doctoralThesis). Universidade do Minho, Guimarães
14. Malhotra, Y., Galletta, D.F. (1999) Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation, 32nd Hawaii International Conference on System Sciences. Maui: IEEE
15. Mandryk, R.L., Atkins, M.S. (2007) A fuzzy physiological approach for continuously modeling emotion during interaction with play technologies. *International Journal of Human-Computer Studies*, *65*(4), 329-347
16. Nickerson, R.S. (1965) Short-term memory for complex meaningful visual configurations: A demonstration of capacity. Canadian Journal of Psychology/Revue canadienne de psychologie, 19(2), 155
17. O'Reilly, C., Chatman, J., Caldwell, D. F. (1991) People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit. Academy of Management Journal, 34, 487-516
18. Paulson, L.D. (2002) Taking a graphical approach to the password. Computer, 35(7), 19-19
19. Reid, J.E., Inbau, F.E. (1977) Truth and deception: The polygraph (lie-detector) technique (2nd ed., Vol. xvii). Williams & Wilkins Co
20. Revett, K., Deravi, F., & Sirlantzis, K. (2010) Biosignals for User Authentication - Towards Cognitive Biometrics?, International Conference on Emerging Security Technologies (EST), pp 71-76
21. Ross, A., Jain, A.K. (2004) Multimodal biometrics: An overview. 12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, 1221–1224
22. Sá, V.J.; Malerczyk, C.; Schnaider, M. (2002) Vision Based Interaction Within a Multimodal Framework. Selected Readings in Computer Graphics 2001, ISBN: 3-8167-6163-1, Fraunhofer IRB Verlag, Stuttgart
23. Shepard, R.N. (1967) Recognition memory for words, sentences, and pictures. Journal of verbal Learning and verbal Behavior, 6(1), 156–163
24. Standing, L. (1973) Learning 10000 pictures. The Quarterly Journal of Experimental Psychology, 25(2), 207–222
25. Stern, R.M., Ray, W.J., Quigley, K.S. (2001) Psychophysiological recording. Oxford University Press
26. Suo, X., Zhu, Y., Owen, G.S. (2006) Analysis and Design of Graphical Password Techniques. Em G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, et al. (Eds.), Advances in Visual Computing (Vol. 4292, pp 741-749), Springer: Berlin, Heidelberg.
27. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N. (2005) Authentication using graphical passwords: effects of tolerance and image choice. Proceedings of the 2005 symposium on Usable privacy and security, SOUPS'05 (pp 1–12). Pittsburgh, Pennsylvania: ACM.
28. Yan, J., Blackwell, A., Anderson, R., Grant, A. (2004) Password memorability and security: Empirical results. Security & Privacy, IEEE, 2(5), 25-31