Odour User Interface for Authentication: Possibility and Acceptance: Case Study

Abdullah Rashed & Henrique Santos

***Abstract*---Historically, some new technologies are faced with rejection or acceptance. So researchers developed TAM (Technology Acceptance Model). TAM depends upon the user perception of the easiness and benefits. Authentication plays an important role in our lives as we use it every day.**

Odour, as a biometric technique, has some important characteristics, mainly, it is faster and easier since users will be not involved with unfamiliar interfaces such as typing password, signing or even deliberate exposing some part of the body. Odour field is still under development and needs a lot of work. In spite of the few limited researches that discuss the odour as user authentication technique their results predict that it would be good tool. This brings a question about the future of odour authentication systems and using it in real world.

A questionnaire was distributed to measure the acceptance of using odour as authentication system and analyzed the collect data. It is concluded that it would be successfully used in authentication systems.

Keywords: ***Biometrics, biometrics technology, Authentication, odour, smell sense.***

I. INTRODUCTION

As we live in the era of digital kingdoms information age, we become computer slaves [18] that makes human life much easier, but not secure [22]. Secure areas are controlled by possession of a particular artifact [7]. For business issues transactions, some organizations provide their services via the Internet [21] and provide some information related to their employees. This kind of services needs focusing on security issues relevant to the clients' side of online banking systems. Information overloading is increased for that reason and due to the applications expansion that need authentication. For individuals it would be difficult to remember their user names and PINs. So many users select easy passwords to remember [7] which are considered a security trade-off.

In response information security is looking for more advanced techniques that would improve its performance. Biometrics introduces good solutions for most of the authentication problems.

There are three types of authentication: [2], [24], [7], [3], [22], [12] and [14]:

Manuscript received January 14, 2010.
Abdullah A. Rashed is with the Research Centre Algoritmi, University of Minho, Portugal (e-mail: rashed@dsi.uminho.pt). Henrique Santos is with the Research Centre Algoritmi, University of Minho, Portugal (e-mail: hsantos@dsi.uminho.pt).

1) *Something you know*, a PIN. 2) *Something you have*: a passport, driver's license, ID card, key, ATM card or cell-phone as suggested by [13]. 3) Something you are (Biometrics): fingerprints, signature, ear shape, odour, keystroke, voice, finger geometry, iris, retina, DNA, hand geometry [20].

The PIN is the most widespread technique, due to its ease of use, but it has an important vulnerability related to the difficulty of humans to memorize several passwords/PINs. So biometrics would be the best solution for that. Users can confirm their personal identity via using biometrics techniques without being asked for PINs also without requiring remembering anything [7] and this makes users more comfortable [22] . Odour or sense of smell is defined the ability of humans and other animals to perceive odours [25]. Smell has a strong link to memory and emotion so it can be good enough to be considered a way to cue recall when searching [4].

Oduor is used by animals to recognize each other. Dogs depend on their noses to smell and determine the direction of the air current containing the smell [26].

Human being sense of smell (odour) is very rich, but not used [4] as this field is under development [16]. So odour field is much less well understood with comparison with face or voice recognition [4]. One of the reasons is that it lacks to the necessary research; in addition to that there are few effective computer controlled smell devices which can discriminate a broad range of odours [4].

Odour as authentication tool would be used in all sensitive organization. However, there can be a problem concerning its acceptance by users.

Customer acceptance is very important as the new technologies might be rejected in unexpected way. The first mechanical cash issuer was installed in 1939 in New York City, but removed after six months. It lacked of customer acceptance [19]. Acceptance of technology is milestone [23]. In this paper, we try to investigate the acceptance of odour as authentication tool.

The rest of the paper is organized as follows. In Section 2; we overview the previous studies as literature review and address the problem statement. In section 3 we demonstrate our methodology and discussion. We conclude and present future work in section 4.

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

II. LITERATURE REVIEW:

In [8], authors focused on the complex problem of authenticating a user; highlighting ethical issues related with authentication mechanisms where it can be made without the collaboration of the users being authenticated. They introduced keystroke dynamics biometrical technology as solution when used in collaborative mode.

[6] discussed consumer acceptance of virtual stores: they presented a theoretical model and critical success factors for virtual stores.

[17] reviewed the literature concerning nine prominent theories and models of authentication and IT acceptance. A questionnaire survey method was used to collect primary data to present Internet Acceptance Model (IAM) and usage by Thai academics. His thesis focused on Internet usage behaviour and behaviour intention.

The questionnaire survey included 927 academics within Business Schools in 20 Public Universities in Thailand and their survey yielded 455 usable questionnaires, with a response rate of 49%. (IAM) is supposed to have the power to explain and predict user behaviour in a Thai Business Schools environment and may help practitioners to analyse the reasons for resistance toward the technology and also help them to take efficient measures to improve user acceptance and usage of the technology.

[1] tried to solve the security problems of online banking using SMS messages for transaction authorizations, by suggesting the SMS authorization scheme. They stated that their solution aimed to stop phishing attack. However, their solution will not stand against the intelligent Trojans which would be installed on the users' client machines via man in the middle attack.

[5] discussed the current security testing categories, standards, and common security testing approaches. Authors thought that the two problems of online banking were: first one is that the online security lacked to the attention and research that should focus on the security issues related to the client side. The second problem related to the huge number of security product that would increase the difficult level to test the category and standards of the security. They presented a scheme to design a compliance testing system for the security of online banking. The presented scheme aimed to obtain suggestions from testers that might help to design security testing and identify potential vulnerabilities in current online banking systems.

[7] addressed consumer-driven usability and user acceptance of biometrics. They focused on how iris can be used with ATM technology user interface. Their findings showed that 90% were satisfied with iris verification method and they would select it over signatures or PINs.

Using odour is introduced as patents in [11], [15] and [10]. In [11], a smell sensing element and a smell sensing device utilizing the element was introduced.

In [15], authors stated that they presented an invention that included an authentication framework in the computer system. An application program interface in the authentication framework was prepared to provide an interface to an I/O component, such as a graphical user interface (GUI), of the computer system.

[11] introduced odour for "A security system checking or transport of persons by an elevator: a person is authenticated by at least one authentication signal. At least one mobile authentication device carried by the person detects an authentication signal of the person and checks it with at least one person reference. The identification code is detected by a stationary recognition device and assigned to a predefined travel destination or to an input travel destination input at the recognition device by the person".

In [16], author overviewed the problem of human recognition through the odour. The electronic nose (ENose) was suggested as an odour recognition device. The model main components of ENoses were presented (see Figure 1).

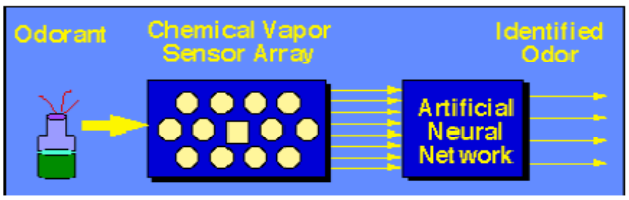

Figure 1: e-nose [16]

Using odour as authentication tool may not be expected by users. The biometric technologies create the challenge of avoiding attacks before they take place [9]. We think that the problem is how we could present the odour in the form that overcomes the worries expectations of users.

III. METHODOLOGY AND DISCUSSION

A bilingual (English and their Arabic) questionnaire was designed and distributed via email to our network contacts. It took days to receive the first response and we used chat to motivate and answer the respondents' notes and questions due to the different languages interpretation and cultural habits. Another reason of misunderstanding was that the topic was too much unexpected for many of them. In the other hand, seventy seven printed papers were distributed and the returned amount was seventy four.

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

So our sample consists of eighty four respondents. The main findings are:

1. Age of the respondents was within the interval [21-30] that represents youth people with 67%.
2. The participants (56 which represents 67%) found it easy to use odour as authentication system.
3. 58% of the participants pointed odour for authentication system as a good idea.
4. They (59 which represents 71%) found odour as authentication system would improve their performance and they (46 which represents 55%) found it would enhance their effectiveness in life.
5. 42% of the participants intended to use odour as authentication system, whereas 10 (1.2%) would not use if it is available.
6. Most of respondents have not ever used odour as authentication system.
7. 17 of those who did not use odour as authentication system reported they did not need to use it. Whereas majority of them (38 represents 46% of the sample and 54% who did not use odour) reported it was not available. Most of them (89 which represents 59%) would use it frequently if it would be available.

By applying TAM model it is expected to accept odour as authentication technology.

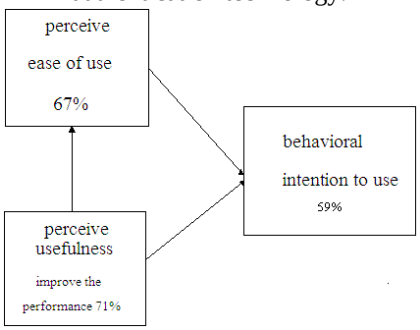

Figure 2: Applying TAM on Odour

IV. CONCLUSION AND FUTURE WORK

We distributed a bilingual questionnaire to study accepting odour as authentication tool. Respondents found it good idea and intended to use it in the future if it is available. We think that odour can be used as an authentication method. Presenting the tool in acceptable form would accelerate the acceptance and adoption of this tool. It is a challenge to apply this approach due to:

1. Acceptance by the customers due to its simplicity: customers have to do nothing whereas people used to apply very complicated authentication depending on the importance of that issue. This would raise the user worries about the security of this approach.

2. Many users thought that hacking this approach would be easy and needs to be strengthening with another approach that enhances it is performance.

The solution is that users who need to authenticate themselves should carry their e-citizen cards. This card should obtain both: Microprocessor that can compare the extracted odour and the biometrics stored information. So the intelligent card can carry out the authentication process.

In addition to that; the card should include storage for storing biometrics data: encrypted digitized format stored in the card.

As future work; a study can be carried out to discover whether there is different between fresh sweat and old one or not.

ACKNOWLEDGEMENT

Authors would like to thank both Ahmed Al-Awthen and Ms. Arwa Al-Eriani for their help.

REFERENCES

[1] AlZomai M., AlFayyadh B., Audun Jøsang A., cCullagh A.(2008), ***An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems***, Proceedings of the sixth Australasian conference on Information security - Volume 81, Wollongong, NSW, Australia , pages:65-73, ISBN ~ ISSN:1445-1336 , 978-1-920682-62-0

[2] Bala D.(2008), ***Biometrics and Information Security,*** Proceedings of the 5th annual conference on Information security curriculum development, Kennesaw, Georgia, ISBN:978-1-60558-333-4, pages: 64-66

[3] Boatwright M., Luo X. (2007), ***What Do We Know About Biometrics Authentication?,*** proceedings of the 4th annual conference on information security curriculum development, Kennesaw, Georgia, Article No. 31 , ISBN:978-1-59593-909-8

[4] Brewster S., McGookin D., Miller C.(2006), ***Olfoto: Designing a Smell-based Interaction***, Proceedings of the SIGCHI conference on Human Factors in computing systems, Montréal, Québec , ISBN:1-59593-372-7, pages: 653 - 662

[5] Chen H., Corriveau J.(2009), ***Security Testing and Compliance for Online Banking in Real-World***, Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I, IMECS 2009, March 18 - 20, 2009, Hong Kong.

[6] Chen L., Gillenson M., Sherrell D. (2004), ***Consumer Acceptance of Virtual Stores: A Theoretical Model and Critical Success Factors for Virtual Stores,*** ACM, Volume 35, Issue 2, pp 8 – 31.

[7] Coventry L., De Angeli A., Johnson G.(2003), ***Usability and Biometric Verification at the ATM Interface,*** Proceedings of the SIGCHI conference on Human factors in computing systems, Ft. Lauderdale, Florida, USA, ISBN:1-58113-630-7, pp: 153 - 160.

[8] De Magalhães S., Kenneth R. Santos H., Sérgio P., Kenneth P., Santos, Santos H. (2006), ***Keystroke Dynamics : Stepping Forward in Authentication***, "GESTS International Transactions on Computer Science and Engineering", .ISSN 1738-6438, pp:29-30.

[9] De Magalhães S., Santos H., De Araújo M., Fangueiro R., Santos A. (2006), ***Wearable Authentication Device with Biometrical Intrusion Prevention System***, *Proceedings* of the *IADIS* International *Conference MULTI* 2005, 11-29 April, 2005. *Lisbon*: *IADIS* Press, 2005.

[10] Friedli P., Gaussmann A. (2005), ***System for Security Checking or Transport of Persons by an Elevator*** , Application number: 10/829,489, Publication number: US 2005/0138385 A1, Filing date: Apr 22, 2004 , Inventors: ,

U.S. Classification 713..., International Classification H04K001/00

[11] Fukui K., Shigemori T., Ehara K.(1989), ***Smell Sensing Element and Smell Sensing Device***, Patent number**:** 5047214, Filing date: Mar 8, 1989, Issue date: Sep 10, 1991, Assignees: New Cosmos Electric Co., Ltd., Primary Examiner: Howard Hampel, U.S. Classification 422/98; 422/96; 422/88; 73/310.6; 338/34, International Classification G01N 2712.

[12] Gleni S., Petratos P.*(2004)*, ***DNA Smart Card for Financial Transactions,*** ACM Crossroads, *Volume 11 , Issue 1, 2004, ISSN:1528-4972,* pages:4 *-8*..

[13] Herzberg A. (2003), ***Payments and Banking with Mobile Personal Devices***, Communications of the AC, Volume 46, Issue 5, 2003, ISSN: 0001-0782, pages: 53 - 58.

[14] Jones L., Antón A., Earp J. (2007), ***Towards Understanding User Perceptions of Authentication Technologies***, Workshop On Privacy In The Proceedings of the 2007 ACM workshop on Privacy in electronic society, Alexandria, Virginia, USA.

[15] Kao I., Milman I., Schneider D., Willard R.(1999), ***Authentication Framework for Multiple Authentication Processes ,*** Patent number: 6651168, Filing date: Jan 29, 1999, Issue date: Nov 18, 2003, , Assignees: International Business Machines, Corp. Primary Examiner: Gilberto Barrn, Secondary Examiner: Doug Meislahn, Attorneys: Morgan & Finnegan, LLP, Joseph C. Redmond, Jr., Application number: 9/240,492, U.S. Classification 713/185; 713/182; 713/155, International Classification H04L 930

[16] Korotkaya Z. (2003), ***Biometric Person Authentication: Odor ,*** available via http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf.

[17] Kripanont N.(2007), ***Examining a Technology Acceptance Model of Internet Usage by Academics within Thai Business Schools,*** PhD thesis , School of Information Systems, Faculty of Business and Law, Victoria University, Melbourne, Australia, available via *wallaby.vu.edu.au/adt-VVUT/uploads/approved/.../01front.pdf*

[18] Lao G., Wang L. (2005), ***Application of E-commerce Security Management Strategy in Banking,*** Proceedings of the 7th international conference on Electronic commerce, Xi'an, China, Pages: 627 – 632.

[19] MIT School of Engineering (2003), ***Inventor of the Week***: **Range Estimation Trainer,** , available via http://web.mit.edu/invent/iow/simjian.html .

[20] Prashanth C. , Ganavi S., Mahalakshmi T. ,Raja K.,Venugopal K., Patnaik L. (2009), ***Iris Feature Extraction Using Directional Filter Bank, for Personal Identification,*** Proceedings of the 2nd Bangalore Annual Compute Conference on 2nd Bangalore Annual Compute, Article No. 6, ISBN:978-1-60558-476-8

[21] Segev A., Porra J., Roldan M.(1998), ***Internet Security And the Case of Bank of America***, Internet security and the case of Bank of America, Volume 41 , Issue 10, 1998,ISSN:0001-0782, pages: 81 - 87.

[22] Sukhai N.(1998), ***Access Control & Biometrics,*** Proceedings of the 1st annual conference on Information security curriculum development, Kennesaw, Georgia, ISBN:1-59593-048-5, pages: 124 – 127

[23] Szajna B.(1996), ***Empirical Evaluation of the Revised Technology Acceptance Model***, Management Science, INFORMS, Vol. 42, No. 1 , pages: 85-92.

[24] Whitman, M., Mattord H., ***Management of Information Security***. Canada: Course Technology (2008).

[25] Wikipedia webpage, 1, (2009), ***Dog***, available via http://en.wikipedia.org/wiki/Dog.

[26] Wikipedia webpage, 2, (2009), ***Recognition***, available via http://en.wikipedia.org/wiki/Recognition

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)