You are who you know: user authentication by face recognition

M Klíma[1], A J Sporka[1,2] and J Franc[3]

[1]Czech Technical University in Prague, FEE
Karlovo nám. 13, 12135 Praha 2, CZECH REPUBLIC

[2]University of Trento, DISI
Via alla Cascata 56/C, Povo, 38100 Trento, ITALY

[3]Sun Microsystems, Inc.
The Park, Building 3, V Parku 2308/8, 148 00 Praha 4, CZECH REPUBLIC

xklima@fel.cvut.cz, *adam.sporka@disi.unitn.it, adam@sporka.eu*, *jakub.franc@sun.com*

ABSTRACT

In this paper, a novel method of authentication based on user-performed identification of known and unknown faces is described. The target group of the method is the elderly users for which the use of traditional techniques, such as passwords, personal identification numbers (PIN), or biometrics is not without problems. The performance of this method and authentication by PIN has been compared in a two-pass usability study. Our method performed significantly better than PIN. The method is suitable for low-security applications in hospitals and senior houses.

1. INTRODUCTION

One of the consequences of pervasion of the computing equipment is the computerization of household appliances. This enables the producers build devices that provide larger functionality (such as greater level of automation, remote control, or interconnectedness), implement better power-saving strategies, enable better diagnostics, and enable better integration with e-commerce services. Systems, such as serve@home[1] or MS Windows XP Media Center Edition are examples of this trend.

These systems have typically larger requirements on users' ability to use the computing equipment which puts certain user groups into a disadvantage. At least a basic experience with handling the ICT is often necessary to perform even the simplest tasks. This puts novice computer users into a great disadvantage.

There are numerous initiatives addressing these issues. One of them is the project i2home[2]. Its tag line is "the intuitive interaction for everyone with home appliances based on industry standards". One of the target groups of the project is the elderly people (65+).

The elderly users are a user group facing a number of challenges that make the usage of mainstream technology difficult. To this day, many of them have never used any computer-based technologies. We assume this will improve in the future when today's computer-literate middle generation grows older. However, the certain special needs will remain with the elderly people due to their mental skills and eventually physical limitations (vision, hearing, motor abilities).

In our work we have focused on user authentication techniques suitable for elderly people. We consider easy-to-use but robust and secure user authentication as a foundation stone of a further development of complex and feature rich home environments. In the context of i2home, the user is supposed to authenticate before receiving private messages, modify their user profile, etc.

Traditional methods of the user authentication include entering the combination of user name and password and biometric methods such as retinal scans or fingerprint analysis. We believe that for a number of applications in certain medical conditions, the finger or retinal scanning is not possible. We also assume that remembering a password or a Personal Identification Number (PIN) would be difficult for the elderly people.

Nevertheless, there are numerous alternatives available. One of the current topics of research is the use of pictorial information for authentication. Oorschot and Thorpe (2008) present in their article an interesting survey of the topic. Weidenbeck et al (2005) describe a system where the user is required to click on

predefined parts of the picture that are known only to the user. Tullis et al (2005) and Weinshall et al (2004) describe authentication schemes based on selection of pictures previously assigned to the user from those displayed on the screen. A commercial solution *PassFaces* by Passfaces Corporation is based on identifying previously assigned faces to user's account. To identify a face, the user has to select a picture of the face within a 3×3 matrix of faces and repeat this task until a correct sequence of the faces has been entered.

In this paper, we describe a method similar to *PassFaces* and compare the performance of this method and the traditional user authentication by entering PIN.

2. AUTHENTICATION METHOD

Our method also consists of selection of a face from a matrix of faces. The collection of the faces is provided during an initialization phase by the user. Pictures of all people that the user would safely recognize can be used. However, as opposed to *PassFaces*, our method is based on the selection of the *unknown* face from among the known ones that the user has provided. The unknown face is randomly selected from a pool of unknown pictures. This way we do not require the users to memorize new faces in order to be able to perform the authentication.

The user's authentication is successful in case the user can repeat the task three times in a row. By having the user to select the unknown face out of those presented, we make the authentication harder for a potential intruder who is likely to know only a part of the user's friends.

On the other hand this method is less resistant against attacks of a closely related person who has similar knowledge and sphere of friends and family. Great advantage of this method is that it requires only very little cognitive load from the user as recognition of faces is much more natural operation than recalling the PIN.

Our method is very easy to use even by people with little or no computer skills. The only obstacle represents the interaction with the computer during identification of the unknown face. While using mouse or touchpad is difficult for our target group, using a touch-screen proves to be a very natural way of interaction for the elderly people. This fact was proven in a separate research within the i2home project.

The method could be applied in institutions such as senior houses to separate the private and common areas. We heard many complaints from our test participants about lack of privacy in the senior house they suffer from. Discussions of the same problem could be found in numerous references in literature.

Using privacy regulation model (Bell et al, 2001) for explanation of the meaning of home and primary territories we can apprehend our participants dissatisfaction as insufficient control over intruders entering their territories and invasion of their privacy. On the other hand numerous studies acknowledged that feeling of control over the primary territories is closely associated with greater well-being, positive effects on health and more positive feeling about the environment itself (Gifford 1997).

If such institutions as senior houses aspire to provide home for their inhabitants and not just shelter, features such as defensible markers and clear boundaries between primary (inhabitants' own room) and secondary territories (hall, common room) should be provided.

Our system could serve as a low-security feature for room protection in time when the inhabitant leaves the room. And thus it could significantly enhance inhabitants' feeling of control over their rooms when being not present. Our system can be seen as an alternative solution to the traditional (metal) keys as well as the authentication by PIN. After reviewing the inhabitants as well as the senior house staff, we have found out the following:

- Traditional metal key is not the best solution for our target population because of the risk of its loss. Solving problems with lost keys is an unacceptable work overload for already busy senior house staff.
- Many seniors are using PIN code derived from their life experience. These PINs are related to day of birth of their children, date of marriage etc. Such pins are very vulnerable to social based attacks.
- The staff of the senior house reports difficulties with the learning curve of the seniors, problems related to their memory are often causing they forget the PIN. Consequently the staff has to take appropriate actions to reset the PIN.

As a result of these interviews we think the usage of our system would be of a great benefit for both the inhabitants and the staff.

3. FACE RECOGNITION

Human face recognition has recently received significant attention in association with automated face recognition systems engineering. Cognitive processes underlying face recognition are acknowledged as highly effective. Remarkable is first of all human ability to recognize familiar faces over varying conditions such as varying angle of view, as well as distance, illumination and even degraded depiction (Sinha et al 2006). Understanding such mechanisms is expected to afford useful hints for development of face recognition automated system.

Face developed important role in holding the information about social identity throughout the evolution of human. Ability to identify others immediately and correctly has become crucial for individuals' functioning in diversified society. Face as an instrument for holding extensive social information provides the most important clues for recognizing the others properly.

Research findings of developmental psychology also stress the exceptional role of face recognition among the other higher cognitive processes. Numerous research studies proved the infants' ability to differentiate familiar faces from the other faces as well as visual preference of structures holding traits that are inherent to faces. The most apparent example is the striking ability of neonates to discriminate mother's face from the others (Pascalis et al, 1995). However the effort of developmental researchers is not limited only to infants.

The fact that face recognition abilities stay fairly preserved in old age even when suffering from senile dementia (Ferris et al, 1980) suggests that the face recognition-based authentication seems to be suitable for our target population. Loss of memory as well as many other cognitive abilities observed in aging people does not affect face recognition so significantly, especially when talking about recognizing faces that were learned in preceding stages of life.

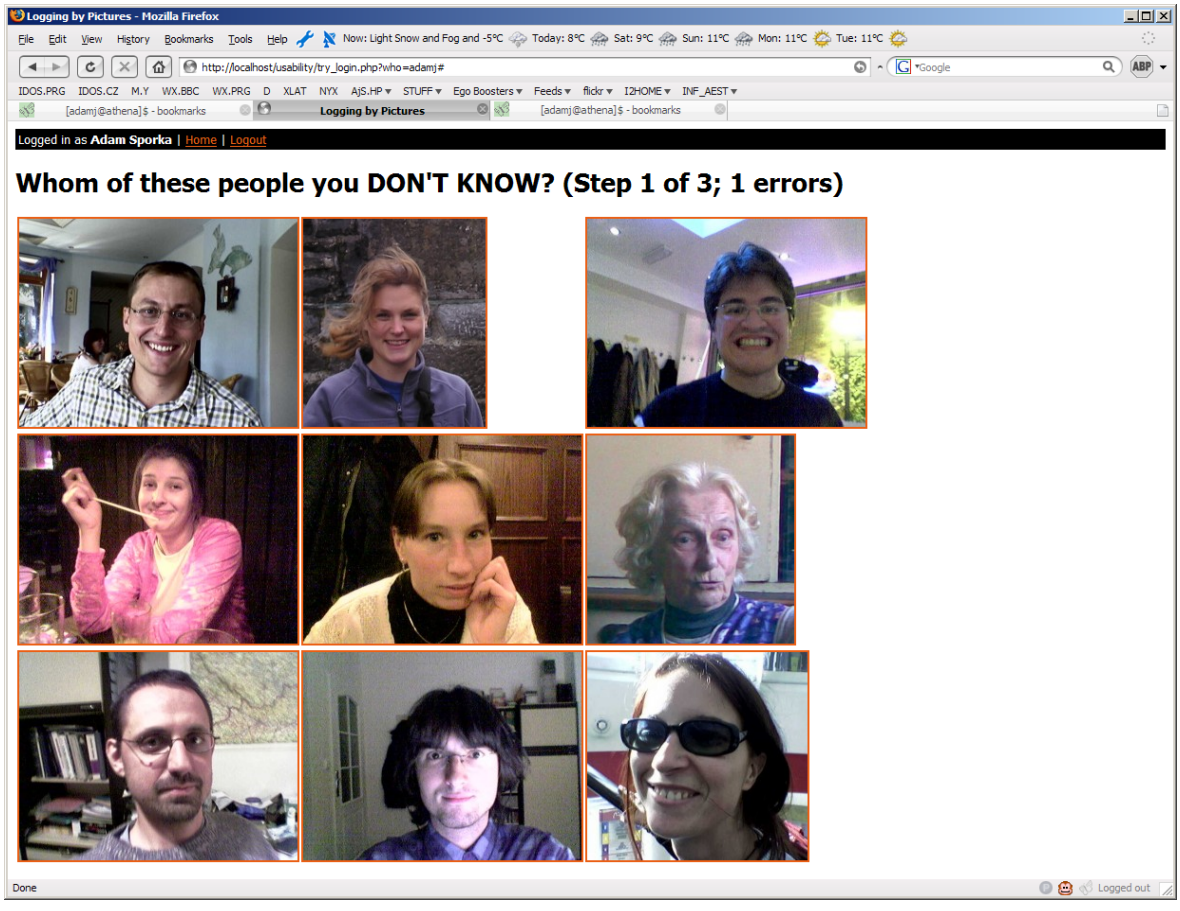

Figure 1. *Screenshot of the authentication prototype tool.*

4. USER STUDY

The goal of this study was to assess the usability of the method that has been developed and to provide a comparison of the method with a commonly used authentication by PIN. The hypothesis of the study was that the log-in by pictures would be more successful than the log-in by PIN, i.e. that there will be more successful authentication attempts by the users when using the log-in by pictures.

4.1 Design

The study was a two-condition within-subject design with repetition.

4.2 Apparatus

A web browser-based prototype application had been written in PHP (Fig. 1.), using Apache HTTP server and MySQL database. The prototype allowed a simple participant management, uploading and automated resizing of the images, and performing the authentication attempts.

During our experiment we instructed the participant to identify the unknown faces by touching a regular LCD screen, the actual selection was made by the experimenter using mouse.

4.3 Participants

There were 9 participants of this study, all females (74 years old, SD 4.2). They all were inhabitants of a senior house located near Prague. The gender of the participants could not be balanced due to the gender profile of the senior house.

4.4 Procedure

The inhabitants of the senior house were invited by the house staff to take part in our study. All people interested in participating gathered in a common room of the senior house a week before the first day of the experiment. The experimenters explained them the goals of the study and have stressed that their participation in the study would be voluntary. In order to help understanding the task, we asked the participants that to imagine they are trying to open a safety vault. Each participant went through two sessions. Each participant was given a small present.

4.4.1 Session 1. A session with each participant consisted of set-up and the test itself. During the set-up phase, each participant signed a consent form. Then, the participant presented the personal collection of photographs to the experimenters who have scanned and uploaded the pictures into the prototype application. The pool of unknown pictures has been generated from the personal collection of one of the experimenters.

At the beginning of the test, the participant was asked to pick and memorize a 4-digit PIN. To approach the real-world conditions, she was advised that certain passwords (repetition of numbers, simple arithmetic sequences, birthdays, etc.) were not acceptable because of their insecurity, as they could be easily guessed. Then she was asked to use our application to attempt a log-in procedure.

The number of attempts needed to complete the log-in successfully was counted. Immediately afterwards, she was asked to enter the PIN. The number of PIN attempts was also counted. The number of attempts was limited to three in both cases, to simulate the behavior of real-world devices, such as cell phones or ATMs, where upon the third failure, the authentication is escalated.

The session took typically between 30 and 45 minutes to complete.

4.4.2 Session 2. 14 days later, a second session has been carried out with each of the participants. Each participant was asked to use our prototype to log in and then she was asked to produce her PIN number. The number of attempts was recorded for both methods with the limit as during the Session 1. The session typically took between 15 and 20 minutes since no set-up was necessary.

The order of the methods tested during the session was fixed due to organizational reasons. However, it could not have affected the results of the experiment: The participants during any of the sessions did not exhibit any symptoms of fatigue or discomfort. On the contrary: After the Session 2, the participants would generally express a disappointment that our visit was too short. Also, our authentication method does not represent any notable cognitive load to the participants and therefore it could not negatively affect the participants' performance in the PIN authentication task.

4.5 Data and discussion

The performance score of the participants is shown in Table 1 for both sessions. On the session 2, the average score of the PIN method was 1.8. Three out of nine users were not able to complete the task successfully. All users were able to finish the task using the picture-based method. Although the number of the participants is relatively small, the difference of the average grades is significant (two-tailed *t*-test, $p < .05$).

Table 1. *Number of attempts taken by the participants.*

		P1	P2	P3	P4	P5	P6	P7	P8	P9	Avg
Session 1	PIN	2	1	1	1	1	1	2	1	1	1.2
	Pict.	2	1	1	3	1	1	1	1	1	1.3
Session 2	PIN	1	1	1	(f) 4	(f) 4	1	1	(f) 4	3	2.3
	Pict.	1	1	1	1	1	1	1	1	1	1.0

Note: (f) denotes a failure to perform the authentication. (Failure is counted as 4 attempts.)

While the users were able to authenticate via both methods on the first session, three users could not pass the PIN on the second session, while all users were still able to perform the picture authentication. The qualitative interviews revealed that our method was generally perceived as "more satisfying", "friendlier", and "easier-to-use".

During the experiment we encountered one participant who had notable problems with memory. Despite of her problems, she performed very well being able to use our authentication method immediately even during the Session 2. We believe that a usability test on people with memory impairment such as Alzheimer's disease should be performed as this method seems to offer benefit over longer period of time than traditional PIN method.

5. CONCLUSION

This paper has reported on a usability test performed on a method of user authentication by means of recognition of human faces on the photographs. The results prove the usability of this method for our target group.

Nine elderly users with no computer skills took part in this study. All of them were able to use the described picture-based method of authentication whereas 3 people were not able to use the authentication by PIN. This study is limited in number of participants. A larger quantitative study must be performed before any possible deployment of our method.

The method shares some benefits and drawbacks with the biometric methods of authentication: The user needs only the life-long knowledge of faces of their family, friends, and colleagues, the authentication procedure is quick and there is no risk of losing the authentication token (password, swipe card, keys…). However, if the potential attacker carries out an extensive study of the user's social background, the security of this method for that user may be ultimately compromised, unless the user later provides previously "unused" faces.

This can happen especially among the members of the family who are likely to know most of the faces on each other's log-in screen as it would be easy for them to guess the unknown person. Therefore, this method is suitable especially for low-security applications in environments shared by multiple people who in general do not know well each other's social history, such as in the hospitals or senior houses. Immediate follow-up will be therefore a statistical study that will examine the level of this threat.

Acknowledgements: This research has been conducted within the i2home project, FP6-033502, http://www.i2home.org. The authors would like to express their thanks to Sri Hastuti Kurniawan for her comments. Adam Sporka's research at the University of Trento is supported by the European Comission Marie Currie Excellence Grant for the ADAMACH project (contract No. 022593).

6. REFERENCES

P A Bell, T C Greene, J D Fisher and A Baum (2001), Environmental psychology (5th edition). Fort Worth: Harcourt College Publishers.

S Ferris, T Crook, E Clarke, M McCarth and D Rae (1980), Facial recognition memory deficits in normal aging and senile dementia, *J Gerontol,* **35**, 5, pp. 707–14.

R Gifford (1997), Environmental Psychology: Principles and Practice. Allyn & Bacon Boston.

W Moncur and G Leplâtre (2007), Pictures at the ATM: Exploring the usability of multiple graphical passwords. *Proc. CHI 2007*, San Jose, CA, pp. 887–894.

P C van Oorschot and J Thorpe (2008), On Predictive Models and User-Drawn Graphical Passwords. *ACM Trans. Inform. Syst. Secur.* 10, 4, article 17, http://doi.acm.org/10.1145/1284680.1284685.

A A Ozok and S H Holden (2005), Alphanumeric and Graphical Authentication Solutions: A Comparative Evaluation. *Proc HCI Intl. 2005*, Las Vegas, NV, pp. 536–544.

O Pascalis, S de Shonen, J Morton, C Deruelle and M Fabre-Grenet (1995), Mother's face recogniton by neonates: A replication and an extension. *Infant Behavior and Dev*, **18**, 1, pp. 79–85.

Passfaces Corporation: Science Behind Passfaces. *A white paper issued by Passfaces Corp.* Available at http://www.id-arts.com/enterprise/resources/white_papers.htm, retrieved 14 July 2008.

P Sinha, B Balas, Y Ostrovsky and R Russell (2006), Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know About. *Proceedings of the IEEE*, **94**, 11, pp. 1948–1962.

T S Tullis and D P Tedesco (2005), Using Personal Photos as Pictorial Passwords. *Ext Abst CHI 2005*, Portland, OR, pp. 1841–1844.

D Weinshall and S Kirkpatrick (2004), Passwords You'll Never Forget, but Can't Recall. *Ext Abst CHI 2004*, Vienna, pp. 1399–1402.

S Wiedenbeck, J Waters, J C Birget, A Brodskiy and N Memon (2005), Authentication Using Graphical Passwords: Basic Results. *Proc HCI Intl. 2005*, Las Vegas, NV, pp. 399–408.

[1] http://www.servehome.com
[2] http://www.i2home.org