Towards Information Technology Security for Universal Access

Shiran Cohen, Noam Ben-Asher, and Joachim Meyer

Department of Industrial Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel
Deutsche Telekom Laboratories at BGU, Beer-Sheva, Israel
{shirang,noambena,joachim}@bgu.ac.il

Abstract. One way to secure Information Technology (IT) systems is with authentication mechanisms that distinguish between users. Users who differ in their cognitive and motor abilities, cultural background and personal characteristics should be able to operate the IT system including its security features. If system design fails to consider user diversity, users might bypass or disable the security feature, reducing system security. Providing universal accessesibility and acceptability is generally a challenge, especially when dealing with IT security. We present a conceptual model that explores and establishes guidelines for the inclusion of biometric authentication in systems which serve a wide range of users. Aspects of this model were examined in laboratory settings using a task which simulates mobile access to an eBanking system with biometric authentication. Younger and older participants used the authentication mechanism. The age groups clearly differed in their interaction with the IT and the security system. Designing security system for universal access remains a major challenge.

Keywords: Universal access, usability, security, authentication, information technology.

1 Introduction

There are undisputable benefits from the increased functionality, connectivity and ability to collaborate provided by Information Technology (IT). However numerous privacy and security issues also arise and pose threats to IT users. One of the common ways to secure an IT system is by integrating authentication and access control mechanisms into it. These mechanisms aim to distinguish between users and protect the registered user from unauthorized access by other people. Knowledge-based authentication uses a word or phrase shared between the user and the IT security system (i.e. - password), token-based authentication uses a physical token, and biometric authentication relies on the uniqueness of details in a person's anatomy or behavior [4]. As biometric authentication methods mostly rely on the users' physical or behavioral features and these features are always available, they can be considered as highly usable compared to token-based methods in which users need to protect the token from being lost or stolen. Moreover, the user is not required to memorize or

C. Stephanidis (Ed.): Universal Access in HCI, Part I, HCII 2011, LNCS 6765, pp. 443–451, 2011.

acquire new information, and thus memory load and cognitive efforts are low. Cognitive effort refers to the amount of resources the user has to invest when learning and executing a procedure. People try to avoid cognitive effort, even if avoidance might lead to adverse consequences [5].

However, while biometric methods have several advantages, they also have some disadvantages. For instance, an individual's age and occupation (e.g. construction work) may make it difficult to capture a complete and accurate fingerprint image. Some of the issues could relate to the cost of the capturing equipment, and vulnerability and privacy issues. Furthermore, biometric systems might solve problems associated with traditional security methods, but if a hacker manages to compromise a biometric system, the privacy of the individual is permanently compromised, because biometrics do not change over time. This property of biometrics constitutes a serious drawback [14].

Users with greatly different cognitive and motor abilities, cultural backgrounds and personal characteristics operate IT security systems on a daily basis. The usage, context of operation and surroundings differ between systems, users and scenarios. This diversity is challenging when designing an IT security system. Various studies have shown that ethnicity, age and gender may limit the use of biometrics [1]. If the design of a security system does not consider these matters, psychological acceptance of the system will be low and users might try to bypass security features and thereby reduce and compromise their own security. Moreover, users might stop using a system if they fail to access it. This study is a preliminary step in evaluating how different aspects of usability affect younger and older users' acceptance and use of biometric authentication in a simulated IT system. We first describe some of the challenges in providing a universally accessible experimental security system, and then present and discuss our findings.

2 Universal Access and IT Security

One of the main requirements that a modern IT security system must meet is universality. This requirement suggests that almost anybody should be able to use the system [12;2]. However, having the physical capabilities required for using the system does not necessarily mean that people will want to use it (or feel they can use it). Additional limitations can prevent people from using the system; these limitations include the whole society (cultural limitations), a specific group (e.g., older users) or the individual itself (technophobia). If these matters are not considered, universality can be unintentionally violated.

It is possible that with aging, motor and cognitive skills decrease and biometric features gradually change [13]. The physical changes include the loss of the lipid (fat) layer in the skin, making fingerprints worn and difficult to image. Similarly, with age voice changes or turns unstable, making vocal signature identification more difficult. Diminishing cognitive abilities (and in particular memory) can cause difficulties when interacting with security systems, especially when the older users need to memorize passwords or use their biometric features. Other common authentication-related failures include non-readable fingerprints, blind users who cannot register iris images,

or cuts and burns on fingers which can cause a temporary inability to use a fingerprint reader [11].

However, providing universal access might not be enough; users should also universally accept security systems. This concept relates to the extent to which people are willing to accept the security measures in their daily life [12]. Cultural incompatibilities can pose constraints on the acceptability of authentication mechanisms. For example, facial recognition is not suitable in cultures where women hide their faces [11] and biometric authentication does not support family members performing tasks in place of the individual who is registered, a customary behavior in some cultures [9].

Hofstede's [6] model defined five cultural dimensions that quantify differences between national cultures: (i) power distance, (ii) individualism, (iii) masculinity, (iv) uncertainty avoidance, and (v) long-term orientation. Power distance is the extent to which a society as a whole accepts an unequal power distribution among its members. Individualism refers to the relative importance of individuals in a society. Masculinity is the difference between male and female gender roles. Uncertainty avoidance defines the society's tolerance of uncertainty and the unknown and long-term orientation is the time focus of a culture. A study [9] that examined cross-cultural differences in attitudes towards biometric technology in India, the United Kingdom and South Africa found clear differences in the acceptance of different methods. However, the cultural dimensions proposed by Hofstede [6] were not sufficient to explain the differences. The alternative explanation related to the effect of the crime rate in each country. Despite the presented conclusions, Hofstede's cultural dimensions can indeed provide a general framework to investigate a society and her motivation in adopting new technology. However, observing acceptance from the society point of view is not always enough, and there is a need to examine what motivates individuals to adopt new technologies.

The "Diffusion of innovation" tool for assessing technology adaptation was developed by Rogers [10]. It defines five adapter categories that exist in the population: (i) Innovators, (ii) Early adopters, (iii) Early majority, (iv) Late majority and (v) Laggards. One can predict that "innovators'" and "early adopters'" acceptance and thereby interaction and use of IT security can be very different from both "late majority" and "laggards". Moreover, it is likely that "innovators" and "early adopters" are using more advanced services, which create different security needs and include advanced authentication. Additionally, there might be an age difference between the groups - innovators tend to be younger and more technology oriented than the laggards. This assumption is supported by Kowalski and Goldstein [8], who found that the "early majority" are a younger population which responds better to biometric authentication methods, compared with the "late majority" and "laggards".

It is crucial to remember when relating to these models, that they are used to explain adoption of a new technology and do not relate specifically to security systems. Security is a supporting task, as it is not considered as a critical part of the means to achieve a desired goal [11]. Meaning that, it is more sensitive to performance reduction in terms of efficiency, even more than for the production task, on which users are focused. If a supporting task conflicts with a production task, users will attempt to bypass it, maintaining performance in the production task. If a supporting task requires significant extra effort or interferes with the production tasks,

users motivation depend on understanding the reason for this, and have to be incite by a motivator to comply with it. Failure to provide users with the necessary understanding, training and motivation can result in security-related human error. The requirements for a high level of security while maintaining adequate usability and user acceptance are frequently in conflict with each other, and a suitable balance has to be found [3]. Two principles of signal detection theory can be used to assess security and usability of an authentication system, False Match (FM) and False Non-Match (FNM) rates [7]. FM refers to granting access to an unauthorized user due to error in the matching process, FNM refers to incorrectly dismissing an authorized user. Generally, a low FM rate is desired and it indicates a secure system. However, it might lead to higher FNM rate that points to low usability and accessibility that may cause users to avoid the system.

The goal of this study was to identify differences between the young and elderly users when accessing an IT security system. In addition, for each group we observed how the need to authenticate and the authentication process influence the subjective evaluations of the system performance.

3 Method

As previously mentioned, an authentication system has to satisfy a set of usability concerns in order to be adopted and continuously used by users. We developed an experimental environment that includes an eBanking- like investment game combined with fingerprint authentication for this study.

3.1 Participants

The first group of participants included 32 (13 females and 19 males) undergraduate students Industrial Engineering and Management students from Ben-Gurion University of the Negev, with ages ranging from 23 to 28 (mean=25). They received an extra credit point in a course for participation and also had the opportunity of winning a price of 40 NIS based on performance in the task. The second group of participants included 7 subjects (5 females and 2 males) with ages ranging from 55-62. These participants were recruited from the non-academic staff of the university. For participating in the experiment, participants in this group received 50 NIS and the opportunity of winning an additional price of 40 NIS based on performance in the task.

3.2 Apparatus and Procedure

The experiment took place in computer laboratory settings. The experimental system included a personal computer connected to a 17" touch screen and a fingerprint reader (SecuGen Hamster IV). The experimental platform overided the manufacturer properties of the fingerprint reader and controlled the FNM rate of the fingerprint reader and the duration a fingerprint reading was processed before providing a response.

After arriving at the laboratory, each participant signed a consent form and received instructions on the course of the experiment. The investment game had a

touch-screen interface, and an external fingerprint reader was used for the authentication process. During 48 steps of the game, participants could build an investment portfolio by allocating money to different investment channels, differing in their expected profit and the maximal amount of money the user could invest (see Fig. 1.). However, allocating money required prior authentication, after which the participant could transfer money between the investment channels. Alternatively, participants could select to continue with their current portfolio. The incentive to change the portfolio was the opportunity to increase the amount of money invested in channels with a large expected profit and a small variance in the expected profit.

The experimental design was within-subjects with two independent variables and two levels for each variable (four experimental conditions, i.e. blocks, 12 steps each). Participants were randomly assigned to one of eight groups that differed in the block's order. After each experimental block, participants answered questions assessing their subjective experience with the system using a seven-point Likert scales ranging from 'Agree' to 'Disagree'.

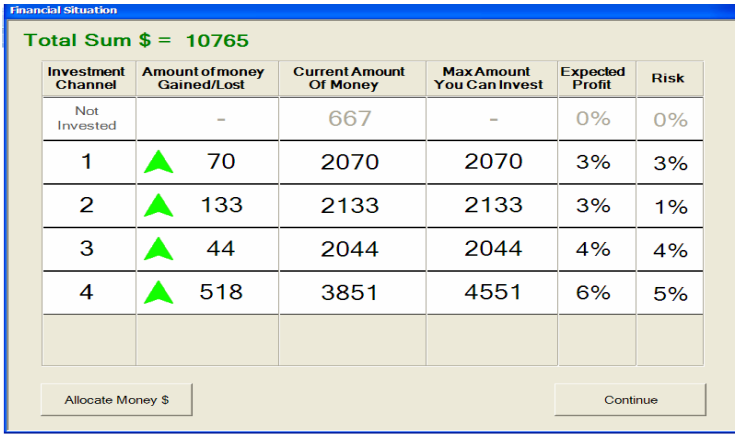

Fig. 1. Screen capture of the investment game

3.3 Independent Variables

The study focused on two independent variables - probability of successful authentication and authentication processing time. The probability of successful authentication was manipulated by changing the number of attempts required to authenticate before the authentication process succeeds. There were two levels of probabilities of success, low and high. When the defined probability for successful authentication is low, participants needed to perform an average of 2.95 authentication trials. For the high probability, the average number of trials until success is 1.5.

The authentication processing time is the time delay from the moment the fingerprint is captured until the system provides the participant with an answer (match or no match). The two levels of time delay differed in their duration, short and intermediate. In the short time delay, after the finger has been scanned and processed

by the system, there is an additional delay of 1 second, and only afterwards a message stating the success or failure of authentication will appear. In the intermediate time delay, the additional delay is 4 seconds. Fig. 2. illustrates the verification process from the moment the user started an authentication attempt until feedback on authentication success or failure was given.

Following each block subjective evaluation of the authentication process was evaluated on three scales. Participants reported their assessment of the reliability of the process, their satisfaction with the interaction with the authentication mechanism and the perceived delay in the processing time.

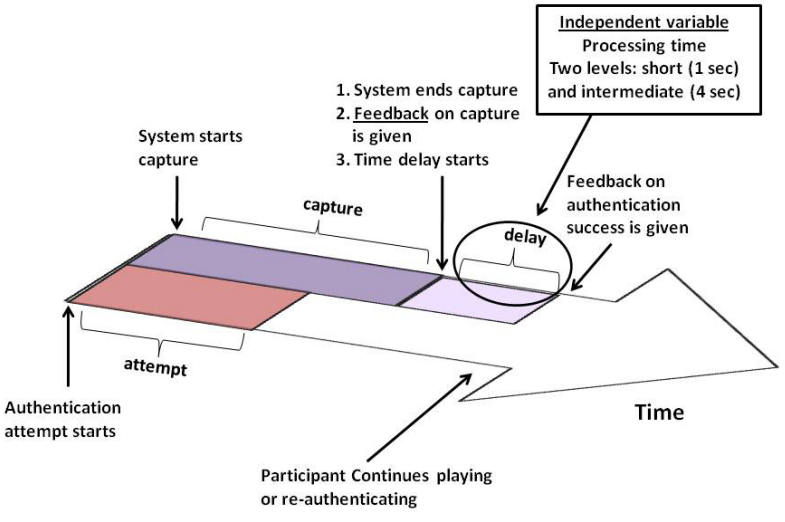

Fig. 2. Authentication process, user and system views

4 Results

The data collected from each group of participants was analyses separately. The effects of the independent variables on the tendency to authenticate was assessed using General Linear Mixed Models, logistic regression analyses and the subjective evaluations of the authentication system were examined using General Linear Models.

4.1 Young Users

The interaction between the probability of a successful authentication and the processing delay had a significant effect on the tendency to authenticate [$z= 3.396$, $p<.01$]. When the delay was short, there was no difference in the rate of authentication attempts between the different probabilities for a successful authentication attempt. However, when the time delay was intermediate, participants in the low probability condition tended to authenticate less, compared with participants in the high probability condition.

The effect of the two independent variables on three subjective measures was examined as well. The results showed that the probability of successful authentication had a significant main effect on the perceived reliability and user satisfaction [$F(1,31)= 7.328$, $p<.01$ and $F(1,31)= 21.691$, $p<.01$, respectively]. As expected, under low probability of successful authentication, the system was perceived as less reliable and thus, users were less satisfied with it. The duration of the time delay had a significant effect on the subjective evaluation of the verification time [$F(1,31)=4.133$, $p<.05$].

4.2 Older Users

Observing the performance of the older users group, we decided to stop the experiment after running only 7 participants. Thus, the results presented here are mainly based on the qualitative observations of the seven participants.

During the experiment, older users asked many questions, interrupting the experimental flow. They needed extensive guidance in order to understand the task and the operation of the fingerprint reader. This turned the first block into learning and training block rather than an experimental block. The older users also had difficulties operating the experimental system with the touch screen as well. This was prominent in two distinct aspects, moving money between channels and selecting whether to authenticate or not. Operating the money transfer between channels took the older users almost twice as long than the young participants group. In addition, the older users complained often about an incorrect selection between authenticating or not. This was repeated in many experimental trials, implying that the quantitative data

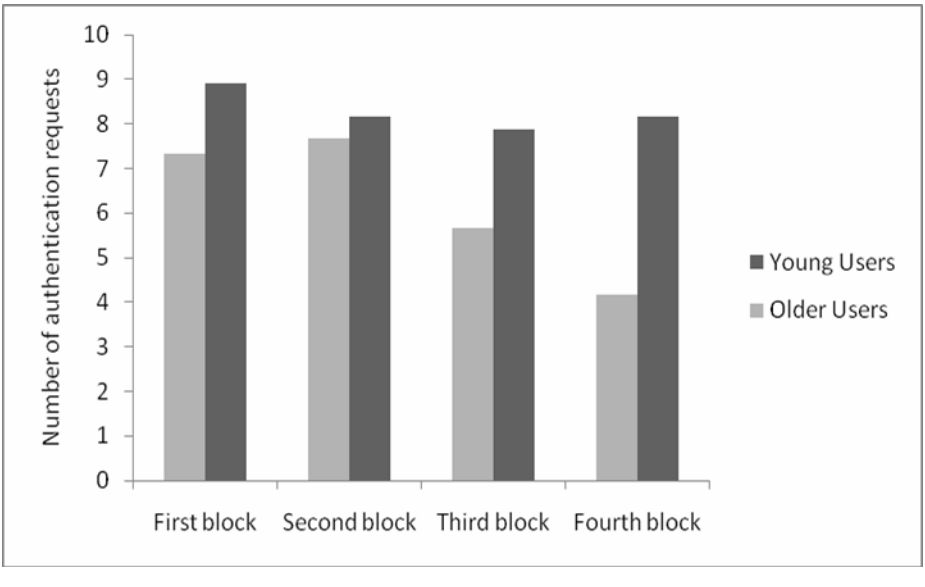

Fig. 3. Average number of authentication requests as a function of experimental block and participant group

on authentication might be biased and may not reflect correctly the decision making process. However, the participants stated that the fingerprint reader was comfortable and that the game itself was the cause of the difficulties.

Furthermore, we observed an effect of the experimental block order on the number of authentication requests that were performed. As seen in Fig. 3., the average number of authentication requests for the young users group is relatively stable over the experimental blocks. However, in the older group participants tended to reduce the number of authentication requests as the experiment proceeded.

5 Conclusions

This experiment is a step towards understanding the variables affecting the adoption and the use of biometric authentication methods. It provides some preliminary understanding of how attributes of an authentication system can influence the tendency to use it by different age groups. The tendency to authenticate was also examined with respect to the reliability and efficiency of the authentication system. Both time delays and system mistakes influenced users' interaction. The probability of successful authentication had a stronger impact on the decisions and assessments of the system functioning than the processing of time delays. A possible explanation could be that the high FNM rate which led to repeated authentication attempts is perceived as a higher cost than the waste of time. Users, especially the older ones, are more tolerant to short delays when using electronic systems. The delays are perceived as a normal part of the system performance. On the other hand, system errors, false non-match mistakes, are perceived as system failures that reduce performance and user trust. Therefore, when considering the universal access to an IT system, one should not distinct between the universal access to the system itself and use of the security system which serves as a gateway to the system. Both should be designed and evaluated in parallel as a condition for successful implementation.

References

1. Ashbourne, J.: Practical Biometrics: From Aspiration to Implementation. Springer, London (2004)
2. Braghin, C.: Biometric Authentication. Technical Report, Department of Computer Science, University of Helsinki (2000)
3. Braz, C., Robert, J.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conference of the Association Francophone D'interaction Homme-Machine, IHM 2006, Montreal, Canada, April 18-21, vol. 133, pp. 199–203. ACM, New York (2006)
4. Brostoff, S., Sasse, M.A.: Are Passfaces more usable than passwords? A field trial investigation. In: Proceedings of HCI 2000, Sunderland, UK, pp. 405–424. Springer, Heidelberg (2000)
5. Ebert, E.J.J.: The role of cognitive resources in the valuation of near and far future events. Acta Psychology 108(2), 155–171 (2001)
6. Hofstede, G.: Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Sage Publications, Inc., Newbury Park (1984)

7. Jain, K.A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 14(1), 4–20 (2004)
8. Kowalki, S., Goldstein, M.: Consumers' Awareness of, Attitudes Towards and Adoption of Mobile Phone Security. In: Proceedings of the 20 International Symposium on Human Factors in Telecommunication (HFT 2006), Nice, France (2008)
9. Riley, C., Buckner, K., Johnson, G., Benyon, D.: Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & Society 24(3), 295–306 (2009)
10. Rogers, E.M.: Diffusion of Innovations. Free press, New York (1995)
11. Sasse, M.A.: Usability and Trust in Information Systems. Cyber Trust & Crime Prevention Project. University College London (2004)
12. Scheuermann, D., Schwiderski-Grosche, S., Struif, B.: Usability of Biometrics in Relation to Electronic Signatures. EU Study 502533/8. GMD-German National Research Center for Information Technology. Institute for Secure Telecooperation, SIT (2000)
13. Seidler, R.D., Stelmach, G.E.: Reduction in sensorimotor control with age. QuestI. 47, 386–394 (1995)
14. Uzoka, F.E., Ndzinge, T.: Empirical analysis of biometric technology adoption and acceptance in Botswana. Journal of Systems and Software 82(9), 1550–1564 (2009)