Poster: Exploring user perceptions of authentication scheme security

Ann Nosseir
British University in Egypt
El Shorouk City
Egypt
nosseir12@yahoo.co.uk

Sotirios Terzis
Department of Computer and Information Sciences, University of Strathclyde
26 Richmond Street, Glasgow, UK
sotirios.terzis@strath.ac.uk

1. INTRODUCTION

Despite researchers' efforts authentication remains a challenge, as demonstrated by the prevalent use of passwords in spite of their usability and security problems. Although alternatives have been suggested addressing these problems [1], they have failed to gain wide acceptance. It is now recognized that a more comprehensive investigation of authentication schemes is necessary to address the challenge [2].

Research has shown that end-user perceptions and attitudes play a major role in the acceptance of new technologies [7]. However, they have received limited attention in the context of authentication [6, 4]. Studies suggest that authentication schemes are distinct enough to require consideration of a different set of factors, like the perception of their security. They have also shown that the relationship between perceived security and acceptance is not linear [6, 4], i.e. up to a certain level of security increases the acceptability of a scheme, but beyond that higher levels of security undermine it. As a higher level of security typically requires increased user effort, it would seem that a scheme that is perceived too easy to use may not be acceptable by users.

From the above, it is clear that studying the perception of their security is an important aspect of a comprehensive investigation of authentication schemes. In this context, we conducted a first study of how users perceive the security of five authentication schemes.

2. STUDY DESIGN

The aim of our study was to see whether schemes with similar security assessment are perceived differently by users and to gain some insight on the reasons behind any differences. The first challenge was to identify the schemes to use, as there are no widely accepted criteria for the assessment of authentication schemes [2].

Bonneau et al. have made a first attempt at developing a set of criteria [1]. They suggest three assessment dimensions, usability, deployability and security. Deployability is not really relevant for end-users, so we do not consider it further. Within each dimension there are a number of desirable properties identified. For example, in security there are properties like resilience to targeted impersonation, explicit consent, unlinkability, etc. While in usability there are properties like nothing to carry, infrequent errors, etc. The assessment is qualitative based on whether a scheme possesses or not the property. Although the assessment is coarse-grained, it has been used to assess a wide range of web authentication schemes. So, we decided to base our choice of schemes on [1]. We started with passwords due to their widespread use and selected schemes with similar security properties to them. The chosen schemes were Pass-Go, GrIDSure, Word associations (WA) and Personal knowledge questions (PKQ) (see [1] for references). They all have resilience to theft, no trusted party involvement, explicit consent, and unlinkability, but differ in resilience to targeted impersonation. Pass-Go and GrIDSure are resilient, password is somewhat resilient, and PKQ and WA are not. It is also worth pointing out that our selection includes schemes from a range of categories; Pass-Go is graphical, GrIDSure and WA are cognitive, and PKQ is a recovery scheme.

Although passwords and PKQ are widely used, the rest are not. So, it was essential that participants experience all schemes. Authentication schemes typically require user involvement in two stages, registration and authentication, and for some of them both stages determine the overall security strength. For example, it is common for passwords to have registration policies restricting user choice, like a minimum acceptable length or a requirement to combine lower and upper case letters, etc. We decided that participants should experience both registration and authentication through a web interface in accordance to [1].

This proved challenging, as the details of their implementation were not clear in all cases. For example, in PKQ a range of questions is used in practice [3, 5]. Rabkin has collected and analysed a set of commonly used questions [3]. We used them to drive our implementation. We started with the question "what is your mother's maiden name", as the "defining" one for the scheme, and the most commonly used questions. However, the applicability of some of them was limited. So, we decided to use five questions in total, three widely applicable ones that were fixed (what is your mother's maiden name, your date of birth, your favourite sport team), while for the other two a choice out of three was given to participants (what was the name of your first pet, make of your first car, your childhood hero, and what is your favourite book/movie/song). Note that selected options have been assessed similar in security strength [3, 5].

In addition to that participants had to answer a number of questions, for biographical information, and for each scheme they had to assess its security using a five point Likert scale ranging from very insecure to very secure, and could justify their assessment. We decided to integrate the questions and the scheme simulations into a single web-based system.

3. STUDY PROCEDURES AND RESULTS

The study was carried out in a computer science laboratory at the British University in Egypt. The participants

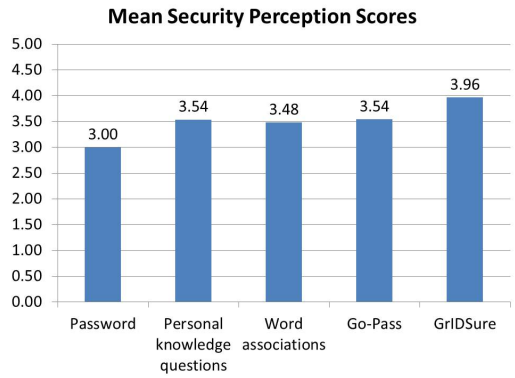

Figure 1: The mean security perception scores for the five schemes.

were all second year students of computer science around 20 years old. There were 42 participants, 27 male and 15 female. Of the 42 responses, 39 were valid for analysis.

Figure 1 shows the mean security perception scores for the different schemes. Although they are fairly close together they are indeed different. Looking closer into the data reveals that only 9 (approx. 43%) participants assessed the security of all five schemes the same, in all cases as "Secure". Based on the security assessment in [1], one would expect password to score higher than WA and PKQ, but it does not. As one would expect, GrIDSure scores higher than PKQ, WA and password, but also higher than Go-Pass. While Go-Pass scores higher than WA and password as one would expect, but surprisingly the same as PKQ. The difference between schemes was statistically significant as determined by one-way ANOVA ($F(4, 138) = 3.068, p = 0.019$). Turkey HSD analysis indicates that the difference between password and GrIDSure is statistically significant at $p < 0.05$. So, we conclude that the security of schemes with similar security assessments can in fact be perceived differently by users.

Looking into the comments provided, we observe that guessability is referred to quite often. This shows that participants do appreciate that schemes belong in the "something you know" category where it is a major issue. References are both positive (e.g. *"it is hard for someone to guess the word you associated"*, or *"[A Go-Pass pattern] is difficult to guess"*), and negative (e.g. *"some passwords are easily guessed"*, or *"anyone can guess what the [associated] words are"*), sometimes for the same scheme (WA). We also observe that personal information is perceived as secure (e.g. *"very personal information is difficult to figure out by [attackers]"*, or *"[associated words] are very personal and cannot be expected"*). This is in contrast to amassing evidence to the contrary and indicates a blind spot for the associated threat. We also observe that familiarity with a scheme affects its perception, either by being more aware of its weaknesses, or by considering it more secure because of its use. Password falls in the former and this seems the main reason behind its relatively low score (e.g. *"a hacker can brute force [a password]"*, or *"[it is not secure] as the length of the password is not specified"*). PKQ falls in the latter (e.g. *"allow the user to recover his account if it is hacked"*). We also observe that effort can positively affect the perception of security (e.g. *"[word associations are very secure because they] take a lot of effort to [register]"*, *"[word associations are secure because they] are hard for the user to memorize"*, or *"[GrIDSure is secure] as it needs more physical effort"*). At the same time, poor memorability is referred to in poor assessments (e.g. *"[word associations are insecure] because you can simple forget the words"*, or *"[Go-Pass is insecure because] the sequence of colour could be easily forgotten"*, or *"[GrIDSure is neither secure or insecure because] it is difficult for the person to remember"*). These results are partly expected and identify aspects like registration or authentication mental effort as factors for further exploration.

We should point out that our conclusions above should be considered with some caution. The number of participants in our study was not very large, and the group was fairly homogeneous, in terms of age and educational background.

4. CONCLUSIONS

We have carried out a first study of how the security of password, PKQ, WA, Go-Pass and GrIDSure are perceived by users. In order to conduct this study we had to address a number of methodological challenges. From our results we conclude that the perception of security does not fully match the reality, and that although guessability is a major contributing factor for "something you know" schemes, it is definitely not the only one, awareness of the potential threats and effort involved also play a role. In the future, we plan to investigate gender differences, and different use contexts like online banking, social networking, etc., as well as different methodological approaches to explore the relationship between effort and perceived security.

5. REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE Symposium on Security and Privacy*, pages 553–567. IEEE Computer Society, 2012.

[2] C. Herley and P. C. van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, 10(1):28–36, 2012.

[3] A. Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of facebook. In L. F. Cranor, editor, *SOUPS*, ACM International Conference Proceeding Series, pages 13–23. ACM, 2008.

[4] J. Rämänen. Perceived security in mobile authentication. Master's thesis, August 2011.

[5] S. Schechter, A. J. B. Brush, and S. Egelman. It's no secret. Measuring the security and reliability of authentication via "secret" questions. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP '09, pages 375–390, Washington, DC, USA, 2009. IEEE Computer Society.

[6] J. Sun and P. Ahluwalia. How users respond to authentication methods: A study of security readiness. In I. Benbasat and A. R. Montazemi, editors, *AMCIS*, page 44. Association for Information Systems, 2008.

[7] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis. User acceptance of information technology: toward a unified view. *MIS Q.*, 27(3):425–478, Sept. 2003.