Towards Improving the Memorability of System-assigned Random Passwords

Mahdi Nasrullah Al-Ameen, Kanis Fatema, Sonali Marne, Sadia Ahmed, Sovantharith Seng, Matthew Wright, Shannon Scielzo
The University of Texas at Arlington
Arlington, TX, USA
{mahdi.al-ameen, kanis.fatema, sonali.marne, sadia.ahmed78, sovantharith.seng }@mavs.uta.edu, mwright@cse.uta.edu, scielzo@uta.edu

Introduction. Given the choice, users produce passwords reflecting common strategies and patterns that ease recall but offer uncertain and often weak security. Addressing this usability-security tension in user authentication remains the key research issue in password studies for decades. In our research, we aim to understand how humans' cognitive abilities could be leveraged to design more secure and memorable authentication schemes. To achieve this goal, we draw upon multiple theories from cognitive psychology and implement them in the context of improving memorability for system-assigned random passwords.

In this workshop, we would provide a clear picture on our findings about the impact of memory cues and user interaction on the memorability of system-assigned passwords. We have conducted several studies in last three years including both lab and field studies on different populations that accommodate young and senior users. The findings from our studies are promising and the experiences are worth sharing [1]. Below, we provide an overview of our major contributions in improving the memorability of system-assigned random passwords:

CuedR [3]. We argue that while the system assigns random passwords, it should also help with memorization and recall. We investigate the feasibility of this approach with *CuedR*, a novel *cued-recognition* authentication scheme that provides users with multiple cues (*visual*, *verbal*, and *spatial*) and lets them choose the cues that best fit their learning process for later recognition of system-assigned keywords. The use of cues facilitates a detailed encoding that helps to transfer the authentication information (e.g., assigned images) from the working memory to long-term memory at registration [4], helping users recognize their images when logging in later. In our study, we found a 100% memorability for CuedR over the span of one week, and 84% of participants preferred to use it in real life as a replacement to traditional textual passwords.

The Impact of Cues and User Interaction on Graphical Recognition [1]. The lab study on CuedR showed promise for providing multiple cues to aid recognition, however, the study did not examine the individual impact of each cue. Thus, we performed this study to explore deeper into this issue, where we examined the efficacy of each individual cue.

We also evaluated the impact of requiring user interaction at registration, in which we have users apply their observation and imagination to type a short description about assigned images. In the course of such observations and thinking on the assigned images, users get more familiar with them and consequently succeed to recognize those images from the set of decoys during login. This process engages users' action-event memory [5], in addition to their visual memory [6], and aids in the elaborate encoding of the authentication secret in long-term memory [4].

In this study, our schemes offer 20 bits of entropy, where the user is assigned five images at registration and has to recognize each of the assigned images from a distinct portfolio of 16 images during login.

The commercially deployed Passfaces scheme uses face images instead of object images, and it is unclear which should be used. We examined this issue in our study. Considering both human faces and objects as images, along with cues and interaction, we designed seven different study conditions. In our within-group study with 56 participants, every participant was assigned seven different graphical passwords, each representing one study condition. One week after registration, participants had a 98% login success rate for a scheme, *ObjectSV* offering users with spatial and verbal cues for object images, while the scheme based on user interaction had a 95% login success rate for face images and a 93% login success rate for object images. All of these were significantly higher than the control conditions representing existing graphical password schemes. The major findings from this study include:

- Verbal cues make a significant contribution in improving the memorability for object-recognition-based graphical passwords.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

[1]Our findings have been published in CHI 2015 [3], SOUPS 2015 [1], and ESORICS 2015 [2]. The findings from our lab study on senior users and the results of our field study are currently awaiting submission. At present, we are working on a large-scale study for senior users and people with learning disability.

- Spatial cues do not contribute significantly to improve memorability for either face or object recognition.
- User interaction is an effective approach to enhance memorability for both face and object recognition.

The Impact of Cues on Textual Recognition [2]. While verbal cues made an important contribution in improving the memorability for system-assigned graphical passwords, we conducted another study to examine the impact of verbal cues in enhancing the usability for textual recognition. To achieve the goal, we designed a scheme, *TextV*: **Text**ual Recognition with **V**erbal cues, and compared it with the *Control* condition that requires users remembering the assigned keywords without the help of verbal cue. In addition, we aimed to understand whether adding images related to the keywords contributes to higher memorability than when users are provided with just verbal cues. So, we designed another scheme, *GraphicV*: **Graphic**al Recognition with **V**erbal cues, and compared it with the TextV scheme [2]. To the best of our knowledge, no study yet has compared textual and graphical recognition-based schemes in terms of usability. In our within-group study with 52 participants, every participant was assigned three different passwords, each representing one study condition. The major findings from our study include:

- In contrast to the suggestion of Wright et al. [7], keeping the position of keywords fixed in a portfolio (i.e., offering spatial cues) did not provide a satisfactory login success rate for textual recognition (61.5%).
- Verbal cues made a significant contribution in improving the login success rate for textual recognition (94.2%).
- Despite the *picture superiority effect* [6], we found no significant difference between textual and graphical recognition in terms of login success rate when both conditions included verbal cues.
- We did find, however, a significant improvement in login time for graphical recognition as compared to textual recognition, even though the number of attempts for successful logins did not differ significantly between these conditions.

Field Study. Based on the findings from these lab studies, it is clear that GraphicV (i.e., ObjectSV) scheme offering users with spatial and verbal cues for object images performed best in terms of memorability. So, we conducted a field study to further examine the usability of this scheme in a real-life scenario. Although a field study is challenging to perform because of the resources and time required, they offer strong ecological validity and the best measure of login performance in a realistic setting. We conducted a 74-day-long field study, including 1349 login sessions from 54 participants. Our results show that GraphicV scheme offered satisfactory memorability in our real-world context, with an overall login success rate of 98%.

Since the prior field studies on system-assigned graphical passwords did not present a detailed analysis of the training effect, it remains of particular interest to the research community to learn how login performances change over login sessions in a long-term field study. We give an insight into this issue by examining the training effect on the usability of our scheme, where we identified an overall improvement in login performance with more login sessions, including a 81% reduction in median login time to just 7 seconds by the 17^{th} login session.

Study on Senior Users. In our studies noted above, most of the participants were young. So, it remains a question of interest that how our scheme would work for people from different ages. Thus, we evaluated the usability of GraphicV scheme for senior users through a pilot study with eight participants (mean age: 80). We found that seven of the participants returned in the login session one week after registration and all of them were able to log in successfully with our scheme.

For this study, we made some important changes in our scheme based on the literature from Cognitive Psychology on senior users. For example, we added *audio cue* to our scheme, which has been found very effective for our participants. With such promising results in this pilot study, we now plan to conduct a large-scale study on senior users. In addition, we are now working on evaluating the usability of our scheme for people with learning disability.

Conclusion. Existing password systems fail to fully address users' cognitive limitations or leverage humans' cognitive strengths. Thus, despite a large body of research, it still remains a critical challenge to build an authentication scheme that provides both guessing resilience and high memorability. Our studies represent a breakthrough, offering high memorability for system-assigned random passwords, and show a promising research direction to leverage humans' cognitive abilities for user authentication.

[2]GraphicV scheme is same as the ObjectSV scheme

1. REFERENCES

[1] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[2] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo. Leveraging real-life facts to make random passwords more memorable. In *ESORICS*, 2015.

[3] M. N. Al-Ameen, M. Wright, and S. Scielzo. Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In *ACM Conference on Human Factors in Computing Systems (CHI)*, 2015.

[4] C. R. Atinkson and M. R. Shiffrin. Human memory: A proposed system and its control processes. *K.W. Spence and J.T. Spence (eds), Advances in the psychology of learning and motivation, New York academic press*, 1968.

[5] M. Knopf, A. Mack, S. Lenel, and S. Ferrante. Memory for action events: Findings in neurological patients. *Scandinavian Journal of Psychology*, 46, 2005.

[6] A. Paivio. *Mind and Its Evolution: A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J., 2006.

[7] N. Wright, A. S. Patrick, and R. Biddle. Do you see your password? Applying recognition to textual passwords. In *SOUPS*, 2012.