Information & Computer Security

Leveraging autobiographical memory for two-factor online authentication

Mahdi Nasrullah Al-Ameen S.M. Taiabul Haque Matthew Wright

Article information:

To cite this document:
Mahdi Nasrullah Al-Ameen S.M. Taiabul Haque Matthew Wright , (2016),"Leveraging autobiographical memory for two-factor online authentication", Information & Computer Security, Vol. 24 Iss 4 pp. 386 - 399
Permanent link to this document:
http://dx.doi.org/10.1108/ICS-01-2016-0005

Received 22 January 2016
Revised 12 April 2016
7 June 2016
Accepted 1 July 2016

Leveraging autobiographical memory for two-factor online authentication

Mahdi Nasrullah Al-Ameen
Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, Texas, USA
S.M. Taiabul Haque
School of Computer Science and Mathematics, University of Central Missouri, Warrensburg, Missouri, USA, and
Matthew Wright
Department of Computer Science and Engineering, University of Texas at Arlington, Arlington, Texas, USA

Abstract

Purpose – Two-factor authentication is being implemented more broadly to improve security against phishing, shoulder surfing, keyloggers and password guessing attacks. Although passwords serve as the first authentication factor, a common approach to implementing the second factor is sending a one-time code, either via e-mail or text message. The prevalence of smartphones, however, creates security risks in which a stolen phone leads to user's accounts being accessed. Physical tokens such as RSA's SecurID create extra burdens for users and cannot be used on many accounts at once. This study aims to improve the usability and security for two-factor online authentication.

Design/methodology/approach – The authors propose a novel second authentication factor that, similar to passwords, is also based on something the user knows but operates similarly to a one-time code for security purposes. The authors design this component to provide higher security guarantee with minimal memory burden and does not require any additional communication channels or hardware. Motivated by psychology research, the authors leverage users' autobiographical memory in a novel way to create a secure and memorable component for two-factor authentication.

Findings – In a multi-session lab study, all of the participants were able to log in successfully on the first attempt after a one-week delay from registration and reported satisfaction on the usability of the scheme.

Originality/value – The results indicate that the proposed approach to leverage autobiographical memory is a promising direction for further research on second authentication factor based on something the user knows.

Keywords User authentication, Autobiographical memory, Usable security

Paper type Research paper

1. Introduction

Traditional textual passwords alone are not adequate to provide security guarantees for online authentication (Council, 2005; J.G.S.IT, 2011), because of attacks such as online guessing, phishing, shoulder surfing and keylogger malware. Thus, it is now widely held that two-factor authentication should be implemented to provide a higher level of

Information & Computer Security
Vol. 24 No. 4, 2016
pp. 386-399
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-01-2016-0005

security (Council, 2005; J.G.S.IT, 2011). For example, the Federal Financial Institutions Examination Council has recommended two-factor authentication for consumer online banking services (Council, 2005). Compliance is also driving adoption of two-factor authentication in other areas, such as the Heath Insurance Portability and Accountability Act in health care (J.G.S.IT, 2011).

1.1 Background and motivation

There are three main types of authentication factors:

(1) knowledge factors (e.g. passwords and PINs);

(2) possession factors (e.g. ID cards and tokens); and

(3) human factors or biometrics (e.g. fingerprints), where knowledge factors are used for authenticating to most online accounts (Council, 2005).

Usually, a traditional user-chosen textual password makes the first component of two-factor authentication for online accounts, whereas the second component varies for different systems.

Some commercial sites send a random, one-time code through text message (short message service – SMS) to be entered by the user, in addition to the user's password (De Cristofaro *et al.*, 2013). Although this approach is widely deployed, it has significant drawbacks. First, although cell phones are very widespread, 8 per cent of US adults do not own one as of August 2015 (Rainie and Zickuhr, 2015). For users with cell phones, a non-trivial fraction of SMS messages is delayed for several minutes or even lost (Meng *et al.*, 2007), and cellular coverage may be poor when they are logging in. SMS messages are not free for all mobile plans, which can discourage adoption. Further, an attacker who gets access to the user's mobile device might be able to learn the user's login information via the phone's browser history and auto-fill features and access the code sent via SMS when attempting to log in.

In a slight extension of the SMS approach, some Web services use a smartphone app to generate one-time code for two-factor authentication. However, around one-third of US adults do not own any smartphone as of April 2015 (Smith, 2015) and, thus, cannot use this scheme[1]. Again, the mobile devices can be stolen and typically have weak or no authentication, which could make this scheme a single point of failure for a user who uses his or her smartphone to get one-time codes for logging into different websites.

Alternately, the random code could be sent through e-mail. As with SMS, however, e-mail delivery is neither fully reliable nor always fast (Moors, 2004). Also, access to the user's mobile device might be enough to overcome this approach, as many users are continuously logged into their e-mail. Also, of course, the e-mail service itself cannot use this technique.

A more secure approach is to provide each user with a physical token to generate the random one-time codes in sync with a server. This approach is implemented in some high-security settings with systems such as RSA's SecurID. The extra hardware requirement adds costs and is hard to extend to multiple accounts without creating a "necklace effect", where the user must carry an unwieldy number of tokens.

Although two-factor authentication typically leverages two of the three types of authentication factors mentioned above, it is possible to have two-factor authentication with two knowledge factors. In particular, several commercial sites deploy recognition-based graphical passwords as the second component of two-factor authentication. Passfaces (R.U.P Authentication, 2004; Biddle *et al.*, 2012) is an example of such a scheme. During registration with this scheme, users are assigned four face-images, each from a distinct portfolio of nine images. At login, users are shown the portfolios of images and are required to correctly recognize the assigned images from decoys for a successful authentication. Passfaces is commercially available and deployed by a number of large sites for two-factor authentication[2].

The memorability for Passfaces, however, is not considered satisfactory (Biddle *et al.*, 2012). Further, Tari *et al.* (2006) found that Passfaces is vulnerable to shoulder-surfing attacks, where university students playing the role of shoulder surfers were able to gain 62 per cent of Passfaces authentication secrets (Tari *et al.*, 2006).

A second component for two-factor authentication should, we argue, have the following features:

- guessing resistance;
- variant response feature to offer resilience against phishing, keyloggers or shoulder-surfing attacks; and
- minimal cost so that user should not need a separate communication channel, extra hardware or an increased memory burden (see Section 3 for details).

1.2 Contribution

To achieve these design goals, we propose to leverage autobiographical memory, information that is known to users based on their life experience. In particular, we build a scheme using cognitive questions (e.g. "What is the last name of your favorite teacher from high school?"). Thus, the user does not need to remember new, artificially constructed information for the authentication secret.

Our scheme invokes the answers to cognitive questions in a novel way to create variant response and thereby provide resistance to phishing, keylogging and shoulder-surfing attacks. The scheme asks users to enter a single letter from a given position of each answer, and this effectively composes a string of characters that varies across the login sessions.

We conducted a multi-session lab study to examine the usability of our scheme. We asked participants in our study to answer three cognitive questions which have shown to be sufficient to guarantee reasonable security against guessing by acquaintances (Just and Aspinall, 2009) and which offer a theoretical guessing space of 14 bits (see the next section for details). We found a high login success rate for our scheme in this study, where a week after registration, 100 per cent of our 19 participants were able to log in in the first attempt.

2. Literature review

Our scheme leverages autobiographical memory, information known to users based on their life experience, by applying cognitive questions as cues to help users recall the information from long-term memory.

2.1 Autobiographical memory

Autobiographical memory is categorized based on different criteria (Williams *et al.*, 2008; Piolino *et al.*, 2006; Hyman *et al.*, 1998). For example, considering different levels of authenticity, autobiographical memory is classified as either *copies* or *reconstructions*

(Williams *et al.*, 2008). *Copies* represent vivid autobiographical memories of an experience with a considerable amount of visual and sensory-perceptual detail. *Reconstructions* are autobiographical memories that are not reflections of raw experiences (Williams *et al.*, 2008). Based on the level of detail, autobiographical memory is categorized as either *specific* or *generic* (Williams *et al.*, 2008). *Specific* autobiographical memories contain a detailed memory of a certain event, whereas *Generic* autobiographical memories are vague and hold little detail other than the type of event that occurred (Williams *et al.*, 2008).

Autobiographical memories can be experienced from different perspectives (Piolino *et al.*, 2006). For example, *field* memories are autobiographical memories recollected in the original perspective, from a first-person point of view. On the other hand, *observer* memories represent autobiographical memories that are recollected from a perspective outside ourselves, a third-person point of view (Piolino *et al.*, 2006). Autobiographical memories can also be differentiated into *remember* vs *know* categories. The source of a remembered memory is attributed to a personal experience, whereas the source of a known memory is attributed to an external source, not personal memory (Hyman *et al.*, 1998).

The cognitive questions used in our study are mostly related to the autobiographical memory that could be categorized as *copies*, *specific*, *field* and *remember*.

According to the conceptual model proposed by Conway and Pleydell-Pearce, autobiographical memory is constructed within a self-memory system, which consists of an *autobiographical knowledge base* and the *working self* (Conway and Pleydell-Pearce, 2000). In the autobiographical knowledge base, the information is categorized into three broad areas: lifetime periods, general events and event-specific knowledge (Conway and Pleydell-Pearce, 2000).

Lifetime periods contain thematic knowledge about the features of that period, such as the locations, relationships and activities involved (Conway and Pleydell-Pearce, 2000). Several of our cognitive questions are related to lifetime periods, for example, "What is the last name of your favorite teacher from high school?" *General events* are more specific than lifetime periods, which refer to single representations of repeated events or a sequence of related events (Conway and Pleydell-Pearce, 2000). *General events* group into clusters with a common theme, and the events that fall under the category of first-time occurrences seem to be particularly vivid (Conway and Pleydell-Pearce, 2000). For example, the cognitive question "What was the first place you remember going on summer holiday?" is related to a first-time occurrence. *Event-specific knowledge* represents vivid and detailed information about individual events, often in the form of visual images and sensory-perceptual features (Conway and Pleydell-Pearce, 2000).

The *working self* deals with the cues used to activate the knowledge structure of the autobiographical knowledge base (Conway, 2005). In this case, cognitive questions work as memory cues (Just and Aspinall, 2009), which contribute to this activation. As the activation occurs, users could recall all levels of knowledge from the autobiographical memory (Conway and Pleydell-Pearce, 2000). Thus, leveraging autobiographical memory could be efficacious to aid password memorability, as a user does not need to memorize new, artificial information specifically for authenticating to an online account.

2.2 Cognitive question

Psychology studies (Anderson and Bower, 1972; Kintsch, 1970; Tulving and Watkins, 1973) reveal that it is difficult to remember information spontaneously without memory cues, suggesting that authentication schemes should provide users with cues to aid memory retrieval. The generate-recognize theory Anderson and Bower (1972) explains the effectiveness of cues in aiding memorability. The theory postulates that retrieval is a two-step process. First, in the generate phase, a list of candidate words is formed by searching the long-term memory. Then, in the recognize phase, the list of words is evaluated to see if they can be recognized as the sought-out memory. According to this theory, a cue can help not only in generating a relevant candidate list but also in recognizing the appropriate word from that list. Cognitive questions work as cues to retrieve the corresponding answers from a long-term memory (Furnell *et al.*, 2004; Forget, 2012).

3. System design

A second component for two-factor authentication should, we argue, have the following features:

- *Guessing resistance*: In this, the attacker should not be able to guess the input, for example, the one-time code. The theoretical guessing space should be at least in line with that of commercially deployed schemes for two-factor authentication, such as the 13 bits[3] provided by Passfaces (Biddle *et al.*, 2012).
- *Variant response*: In this, the user enters a different required input at each login. Variant response is a key feature for complementing textual passwords, which remain the same for each login. Changing the required input each time makes it such that stealing the input once – for example, through phishing, keyloggers or shoulder-surfing attacks – is not sufficient to successfully log in as the user in a future session. Many sites especially require two-factor authentication when logging in from unrecognized devices, for example, public terminals (De Cristofaro *et al.*, 2013), where shoulder surfing could be a potential security threat (Biddle *et al.*, 2012; Tari *et al.*, 2006).
- *Minimal cost*: In this, the user should not need a separate communication channel, extra hardware or an increased memory burden. The problems with using SMS, e-mail and token systems should be avoided if possible. Using a knowledge factor, like Passfaces does, offers the advantage of not requiring an extra communication channel or additional hardware, but Passfaces lacks variant response and adds a memory burden for users who we seek to remove.

To achieve these design goals, we leverage autobiographical memory and invoke the answers to cognitive questions in a novel way. Prior works (Just and Aspinall, 2009; Furnell *et al.*, 2004; Schechter *et al.*, 2009) have identified the shortcomings of cognitive questions in terms of usability and security and suggested appropriate measures to address the noted flaws.

In this section, we first describe the factors that we consider to design usable and secure cognitive questions based on the recommendations from these prior studies (Just and Aspinall, 2009; Furnell *et al.*, 2004; Schechter *et al.*, 2009). We then explain how we leverage cognitive questions to design our scheme.

3.1 Usability of cognitive questions

Just and Aspinall (2009) defined three metrics to measure the usability of a cognitive question: applicability, memorability and repeatability. This provides a useful guide to select appropriate questions for our scheme:

(1) *Applicability*: Not every user can effectively answer every cognitive question. Users in our system choose any 3 questions from a set of 20. Furnell *et al.* (2004) found that 20 cognitive questions were sufficient for registration. Our results indicate that the participants successfully chose three questions at registration and had a satisfactory memorability rate after one week.

(2) *Memorability*: Prior work (Just and Aspinall, 2009; Schechter *et al.*, 2009) shows that a user can easily recall the answers of cognitive questions that are related to his or her long-term memory. Selecting such questions ensures that the user does not need to devote much cognitive effort in learning his or her authentication secrets, as they are simply answers that he or she already knows.

Furnell *et al.* (2004) found that confusion between capital and lowercase letters is a prominent reason for making mistakes when answering a cognitive question. We address this by ignoring case in our scheme:

(3) *Repeatability*: Just and Aspinall (2009) indicate that repeatability can be improved by providing users with a fixed format of answers to questions that ask about dates (e.g. 'Feb-05, 1992′, '02-05-1992′ and '02/05/1992′) or locations. To ensure a large guessing space, we recommend avoiding questions that ask for numerical answers, and this includes questions about specific dates. For location-related questions, instead of imposing any specific format on users, we prefer to be more specific with the questions to ensure repeatability. For example, instead of asking a question with "where?", we would rather ask "in what city or town?". We recommend providing a fixed format for the answer to a question in which being specific with the question does not resolve the repeatability issues.

3.2 Security of cognitive questions

The most important security concerns with cognitive questions include user-created questions, guessing by acquaintances and common answers. We address these security issues in the following way:

- *User-created questions*: If users are allowed to freely create their own questions, many users will not choose sufficiently secure questions (Just and Aspinall (2009)). On the other hand, it may create usability concerns for some users if the questions are strictly assigned by the system. Our scheme balances these trade-offs by asking the users to select any three questions from a larger set.
- *Guessing by acquaintances*: Typically, cognitive questions are prone to targeted guessing attacks in which attackers exploit the knowledge about personal information of a user (Just and Aspinall, 2009; Schechter *et al.*, 2009; Rabkin, 2008). One's mother's maiden name and Social Security Number in the USA are particularly well-known examples of such questions.

Just and Aspinall (2009) show that three questions are sufficient to provide reasonable security against guessing by acquaintances, and we thus require three questions:

- *Common answers*: The answers to some cognitive questions are generally common among users. For example, blue or pink may be common answers to the question "what's your favorite color?". Prior studies (Just and Aspinall, 2009; Schechter *et al.*, 2009) have found that carefully selected questions can make common answers less of an issue for most users. The questions for our scheme were selected carefully based on the prior usability and security analyses of cognitive questions (Just and Aspinall, 2009; Furnell *et al.*, 2004; Schechter *et al.*, 2009).

3.3 Design of scheme

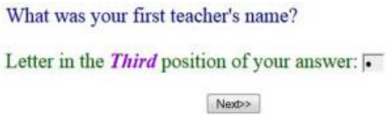
The basic design of our scheme follows a simple and straightforward approach. At the time of registration, the user is shown a set of carefully selected questions (e.g. "what was the first place you remember going on summer holiday?"), of which he or she must select three questions to answer. These answers, in total, constitute his or her authentication secret. During login, a user is asked to enter one letter from a specified position of each answer (Figure 1), and every time a user logs in, this position is randomly chosen by the system individually for each question.

In this way, a user has to correctly enter a letter for each of three questions for a successful login. For example, if a user's answers are: "jimmy" (second), "dhaka" (first) and "manarat" (third), and if he or she is asked to enter the letter at a position given in parentheses, his or her authentication code for this session would be "idn". In a subsequent session, she may have to enter a different code (e.g. "jha") for authentication if the given positions are first, second and fourth, respectively. Thus, varying user inputs across the login sessions (i.e. variant response) creates a distinct code in each session.

During registration, we have deployed some basic restrictions in our system to guard against poor answers (e.g. minimum three characters in an answer, no repeat answers between questions and at least two different letters in an answer) that should have motivated users to enter the correct answer instead of a weak placeholder one ("Aab"). Schechter *et al.* (2009) found that real answers to cognitive questions are more memorable than placeholder answers.

3.3.1 Password space. The questions in our scheme ask users for alphabetical answers (e.g. "what was your first teacher's name?"), where the answers are case-insensitive. During login, the user is asked to enter the character at a given position in his or her answer. In this respect, the size of the domain for an alphabetical entry (26) is larger than that for a numerical entry (10). The theoretical guessing space for this condition will, therefore, be $\log2(26)^3 \approx 14$ bits.

The effective guessing space, which accounts for differences between real answers and random strings, is difficult to quantify without a large study of users' answers. Although Shannon provides a method to compute the entropy of English words



What was your first teacher's name?

Letter in the *Third* position of your answer:

Figure 1.
A screenshot of a demo of our scheme at login

(Shannon, 1951), this method cannot be applied in our scheme. In Shannon's method, the likelihood of guessing the *i*th letter is estimated based on the knowledge of the $(i - 1)$ first letters. In our scheme, however, each input letter in a given code comes from a distinct question and is thus largely independent of the other letters. In this regard, a simple approximation can be developed by using the frequency of letters in English (Young, 2015), even as we recognize that not all questions will have answers with such frequencies. With this approximation, the guessing space for three separate letters is approximately 13 bits, which is in line with Passfaces (R.U.P Authentication, 2004), the commercially deployed two-factor authentication scheme.

Of course, the actual answers do not come from English texts. Actual entropy may be higher or lower depending on the question, the user's background and whether the attacker knows anything about the user or not. A field study would be very interesting to gather a large data set to measure the effective guessing space for our scheme.

3.3.2 Variant response. When the user enters his or her credentials in our scheme, either at registration or login, the answers are shown as asterisks or dots (as with regular password entry) to minimize the risk of shoulder surfing. When a user enters the letter at a given position in his or her answer during login, the shoulder surfer needs to observe both the monitor and keyboard at a time to learn that letter and its position in the answer, which has been found to be difficult in practice (Tari *et al.*, 2006). Even if a shoulder surfer can learn the letter and its position, he or she is likely to be asked to enter a letter of a different position when he or she tries to log in as the user. Only a good guess of the entire answer for all three questions gives the attacker a reasonable chance of logging in. The shoulder surfer may attempt to gain the user's credentials when he or she enters the entire answer to a question at the time of registration. So, we recommend that the users register in a secure environment (e.g. avoiding public terminals) to ensure maximum security.

A system provides resilience against keystroke and mouse loggers (Schaub *et al.*, 2013) when the keyboard/mouse entries for authentication vary across subsequent login sessions (Biddle *et al.*, 2012). Although the traditional textual password does not provide any resilience to keyloggers, our scheme, as a component of two-factor authentication, improves robustness against such attacks through variant response. Our scheme is clearly resilient to mouse loggers, as it does not use mouse input.

In a phishing attack, users are redirected to fraudulent websites to enter their credentials (Biddle *et al.*, 2012). In our scheme, the phishing victim will very likely get different questions from the ones he or she normally uses to log in, as a phisher would not typically have access to the user's login sessions. This means that not only will the user enter information that is useless to the attacker but also the user may be able to realize that something is wrong (i.e. identify a phishing site) and end the session. Further, variant response means that one successful phishing attempt would not be enough to access the account.

4. User study

We performed a user study to get an initial evaluation of the effectiveness of this scheme. The study was approved by our university's Institutional Review Board for human subjects research.

4.1 Participants, apparatus and environment

For this experiment, we recruited 19 university students (4 women and 15 men, mean age = 27 years) from diverse backgrounds, including majors from Biology, Engineering, Interdisciplinary Study, etc. We conducted this multi-session experiment in an isolated room (free from outside noise and distractions) at our university campus. The lab studies were conducted with one participant at a time to allow the researchers to observe the user's interaction with the system. Each participant was compensated with a $10 gift card for participating in this study. Participants were aware that their performance or feedback in this study would not affect the amount of compensation.

To administer this experiment, we created a website with realistic look-and-feel, which was outfitted with our authentication scheme. The website was hosted in a server, which recorded quantitative data (e.g. registration time, login success rate, login time and number of attempts for successful login) to measure the usability of our scheme.

4.2 Procedure

We conducted the study in two sessions, each lasting around 30 min. The second session took place one week after the first one to test memorization of the authentication secret. Note that the one-week delay is larger than the maximum average interval for a user between her subsequent logins to any of the user's important online accounts (Hayashi and Hong, 2011). Also, it is a common interval used in authentication studies (Nicholson *et al.*, 2013; Wright *et al.*, 2012; Al-Ameen *et al.*, 2015c; Al-Ameen *et al.*, 2015a; Al-Ameen *et al.*, 2015b).

4.2.1 Session 1. After signing a consent form, participants registered with the scheme by answering 3 questions out of a set of 20, and these answers constituted their secret. Then, they performed a practice login with our scheme. To motivate users in entering the correct answer instead of a weak placeholder one ("Aab") during registration, we have deployed some basic restrictions in our system to guard against poor answers (e.g. minimum three characters in an answer, no repeat answers between questions and at least two different letters in an answer). In Session 1, the server recorded the registration time, and the user adhered to the basic restrictions while answering the cognitive questions. However, we did not collect data for the login performance of users (e.g. login success rate, login time and number of attempts for successful login) in the practice login trial, as it is a common practice in password studies to examine the memorability of an authentication scheme based on users' login performance after one week of registration, whereas a practice login trial after the registration in Session 1 contributes to compensate for novelty effect (Nicholson *et al.*, 2013; Wright *et al.*, 2012; Al-Ameen *et al.*, 2015c; Al-Ameen *et al.*, 2015a; Al-Ameen *et al.*, 2015b).

4.2.2 Session 2. The participants returned for the second session after one week of registration and logged into the site using our scheme. After they had finished, we conducted an anonymous paper-based survey to get user feedback on the usability of our scheme, where we asked participants to answer a set of ten-point Likert scale questions (1: strong disagreement, 10: strong agreement). Participants were then compensated and thanked for their time.

4.3 Results

As recommended in prior literature (Schaub *et al.*, 2013; Al-Ameen *et al.*, 2015c; Al-Ameen *et al.*, 2015a), we examined the usability of our scheme through login success rate, number of attempts for successful login, registration time, login time and user feedback.

In our scheme, we observed a 100 per cent login success rate on the first attempt after one week of registration. Table I shows the results for registration and login time. The median registration time for the scheme was 52 s, which is deemed reasonable, as it is a one-time cost incurred only during account setup. The median login time for our scheme was 25 s.

Although we have deployed some basic restrictions at registration to guard against poor answers (see Section 3.3 for details), we found that three participants attempted to enter an identical answer for multiple questions at registration, and when they saw the error message, they entered distinct answer for each question.

We asked participants to answer a set of ten-point Likert scale questions (1: strong disagreement, 10: strong agreement) at the end of the second session (Table II). As Likert scale data are ordinal, it is most appropriate to calculate mode and median for Likert scale responses (Robertson, 2011). In our study, user feedback is consistent with the high login success rate, where the feedback of the participants was overall positive about memorability (mode: 9, median: 9) and ease of login (mode: 10, median: 9). They also reported that with practice, they could log in more quickly with the scheme (mode: 10, median: 9). We recognize that social acceptability bias might lead to higher scores in this kind of survey, but the positive results provide mild evidence that the scheme is not overly burdensome for users.

5. Discussion

Based on an extensive survey on 25 different authentication schemes, Biddle *et al.* (2012) identified the features of an ideal password scheme and suggest leveraging pre-existing user-specific knowledge where possible, rather than having users memorize entirely new and/or random information. Their suggestion is in line with our approach, where we leverage autobiographical memory to address the shortcomings of existing two-factor authentication systems. For example, SMS and email-based two-factor schemes may fail, for example, because of poor network coverage, whereas the existing knowledge factor-based scheme (Passfaces) suffers from unsatisfactory memorability

Table I. Descriptive statistics for registration and log in time (in seconds)

Study session	Mean	Median	SD
Registration (Session 1)	58	52	44
Login (Session 2)	26	25	16

Table II. Questionnaire responses for the ability of our scheme

Questions	Mode	Median
Logging in using this scheme was easy	10	9
Passwords are easy to remember in this scheme	9	9
With practice, I could quickly enter my password in this scheme	10	9
I could easily use this scheme every day	10	8
I could easily use this scheme every week	10	9

Note: scores are out of 10

and is vulnerable to shoulder-surfing attacks (Biddle *et al.*, 2012; Tari *et al.*, 2006; Valentine, 1999). The relevance of our scheme for two-factor authentication is four-fold:

(1) Unlike two-factor authentication that relies on SMS, e-mail or a smartphone app, our scheme does not require any additional hardware or communication channel, ensuring reliability and availability. The login time is reasonable compared with waiting for an e-mail or SMS message, which are sometimes delayed.

(2) Our scheme does not impose an additional memory burden on users, as it leverages autobiographical memory, information that is known to users based on their life experience. Thus, the user does not need to remember new, artificially constructed information for the authentication secret.

(3) Compared to the commercially deployed two-factor authentication scheme (e.g. Passfaces), our scheme showed better memorability with similar password space (see Section 3.3.1 for details). As shown in prior study (Valentine, 1999), after a week of registration, 83 per cent of users were able to log in at the first attempt with Passfaces scheme, whereas we found a 100 per cent login success rate at the first attempt for our scheme[4].

(4) Variant response is a key feature for complementing textual passwords, which remain the same for each login. Thus, our scheme offers variant response to increase security against shoulder surfing, basic keyloggers and phishing attacks (see Section 3.3.2 for detailed discussion).

5.1 Limitations and ecological validity

In our study, the participants were young and university educated, which represents a large number of frequent Web users, but may not generalize to the entire population. As the study was performed in a lab setting, we were only able to gather data from 19 participants.

Although we suggest our scheme to be the second component of two-factor authentication for online accounts having the traditional textual password as the first component, our study aims to measure only the usability of the proposed scheme to establish performance bounds for a new scheme and understand the corresponding usability issues.

We note that our results for login time are conservative, as they reflect initial use. A recent study (Al-Ameen and Wright, 2014) has shown that login time can decrease with frequent use of a scheme because of training effects. In future work, we would perform a long-term field study to examine how much the training effect leads to improving the login time over more login sessions.

Although a field study offers superior ecological validity, it requires the researchers to invest large amounts of time and resources (Biddle *et al.*, 2012). In this regard, lab studies have the advantage of being held in a controlled setting and so can be used to discover unexpected usability problems and indicate whether field tests are worthwhile. Now that we have found promising results for our scheme in the preliminary lab study, we plan to conduct a multiple-password field study with a larger and more diverse population, combining our scheme as the second component of two-factor authentication with a traditional textual password.

6. Conclusion

In this paper, we sought a second factor to complement passwords for two-factor user authentication that would not rely on secondary communication channels and not be inherently vulnerable to loss or theft of the user's phone. To achieve this, we leverage the user's autobiographical memory in a novel way to create a distinct code in each login session, providing the advantages of one-time codes together with the advantages of knowledge factors. In particular, changing the required input each time makes it such that stealing the input once – for example, through phishing, keyloggers or shoulder-surfing attacks – is not sufficient to successfully log in as the user in a future session. Our scheme showed promising memorability in a preliminary lab study and, thus, presents an interesting direction for future work on a second authentication factor based on something the user knows.

Notes

1. People who do not own smartphones might use features phones (i.e. that do not run apps). Also, 8 per cent of US adults own neither a smartphone nor a basic cell phone as of August 2015 (Rainie and Zickuhr, 2015).
2. www.realuser.com/ shows testimonials about Passfaces from customers.
3. Bits being the log base two of the number of possible guesses.
4. We note that direct comparison between different studies should be taken with caution.

References

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

Al-Ameen, M.N., Fatema, K., Wright, M. and Scielzo, S. (2015b), "Leveraging real-life facts to make random passwords more memorable", *European Symposium on Research in Computer Security (ESORICS)*, Vienna.

Al-Ameen, M.N. and Wright, M. (2014), "A comprehensive study of the GeoPass user authentication scheme", arXiv preprint, arXiv:1408.2852.

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

Anderson, J.R. and Bower, G.H. (1972), "Recognition and recall processes in free recall", *Psychological Review*, Vol. 79 No. 2, p. 97.

Biddle, R., Chiasson, S. and van Oorschot, P. (2012), "Graphical passwords: learning from the first twelve years", *ACM Computing Surveys*, Vol. 44 No. 4.

Conway, M.A. (2005), "Memory and the self", *Journal of Memory and Language*, Vol. 53 No. 4.

Conway, M.A. and Pleydell-Pearce, C.W. (2000), "The construction of autobiographical memories in the self-memory system", *Psychological Review*, Vol. 107 No. 2.

Council, F.F.I.E. (2005), "Authentication in an internet banking environment", *Financial Institution Letter, FIL-103-2005*, Vol. 18, Federal Deposit Insurance Corporation (FDIC), Washington, DC, p. 2005.

De Cristofaro, E., Du, H., Freudiger, J. and Norcie, G. (2013), "A comparative usability study of two-factor authentication", arXiv preprint arXiv:1309.5344.

Forget, A. (2012), "A world with many authentication schemes", *Ph.D dissertation*, Carleton University, Ottawa, ON.

Furnell, S., Papadopoulos, I. and Dowland, P. (2004), "A long-term trial of alternative user authentication technologies", *Information Management and Computer Security*, Vol. 12 No. 2.

Hayashi, E. and Hong, J.I. (2011), "A diary study of password usage in daily life", *ACM Conference on Human Factors in Computing Systems (CHI), Vancouver, BC.*

Hyman, I.E., Gilstrap, L.L., Decker, K. and Wilkinson, C. (1998), "Manipulating remember and know judgements of autobiographical memories: An investigation of false memory creation", *Applied Cognitive Psychology*, Vol. 12 No. 4, pp. 371-386.

J.G.S.IT (2011), "Understanding the security and privacy rules associated with hitech and hipaa acts, topic: multifactor authentication", White Paper, July.

Just, M. and Aspinall, D. (2009), "Personal choice and challenge questions a security and usability assessment", *Symposium on Usable Privacy and Security (SOUPS)*, *Mountain View, California.*

Kintsch, W. (1970), "Models for free recall and recognition", Norman, D. (Ed.), *Models of Human Memory*, Academic Press, New York, NY.

Meng, X., Zerfos, P., Samanta, Y., Wong, S.H. and Lu, S. (2007), "Analysis of the reliability of a nationwide short message service", *Annual IEEE Conference on Computer Communications (IEEE INFOCOM)*, *Alaska.*

Moors, T. (2004), "Email dependability", *Email Management World.*

Nicholson, J., Coventry, L. and Briggs, P. (2013), "Age-related performance issues for pin and face-based authentication systems", *ACM Conference on Human Factors in Computing Systems (CHI)*, *Paris.*

Piolino, P., Desgranges, B., Clarys, D., Guillery-Girard, B., Taconnat, L., Isingrini, M. and Eustache, F. (2006), "Autobiographical memory, autonoetic consciousness, and self-perspective in aging", *Psychology and Aging*, Vol. 21 No. 3, p. 510.

Rabkin, A. (2008), "Personal knowledge questions for fallback authentication: security questions in the era of facebook", *Symposium on Usable Privacy and Security (SOUPS)*, *Pittsburgh, PA.*

Rainie, L. and Zickuhr, K. (2015), "Americans views on mobile etiquette", available at: www.pewinternet.org/2015/08/26/americans-views-on-mobile-etiquette/

Robertson, J. (2011), "Stats: We're doing it wrong", available at: http://cacm.acm.org/blogs/blog-cacm/107125-stats-were-doing-it-wrong/fulltext

R.U.P Authentication (2004), "The science behind passfaces", White Paper, June.

Schaub, F., Walch, M., Konings, B. and Weber, M. (2013), "Exploring the design space of graphical passwords on smartphones", SOUPS.

Schechter, S., Brush, A.J.B. and Egelman, S. (2009), "It's no secret: Measuring the security and reliability of authentication via 'secret' questions", *IEEE Symposium on Security and Privacy*, *Oakland, California.*

Shannon, C.E. (1951), "Prediction and entropy of printed english", *Bell System Technical Journal*, Vol. 30 No. 1.

Smith, A. (2015), "US smartphone use in 2015", available at: www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Tari, F., Ozok, A. and Holden, S. (2006), "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords", *Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA*.

Tulving, E. and Watkins, M. (1973), "Continuity between recall and recognition", *American Journal of Psychology*, Vol. 86 No. 4, p. 739.

Valentine, T. (1999), "An evaluation of the passface personal authentication system", Technical Report, Goldsmiths College University of London, London.

Williams, H.L., Conway, M.A. and Cohen, G. (2008), "Autobiographical memory", Memory in the Real World (3rd Edition), Psychology Press, London, p. 21.

Wright, N., Patrick, A.S. and Biddle, R. (2012), "Do you see your password? Applying recognition to textual passwords", *Symposium on Usable Privacy and Security (SOUPS), Washington, DC*.

Young, B. (2015), "Foundations of computer security, lecture 35: entropy of english", available at: www.cs.utexas.edu/~byoung/cs361/lecture35.pdf

Corresponding author
Mahdi Nasrullah Al-Ameen can be contacted at: mahdi.al-ameen@mavs.uta.edu