Routledge
Taylor & Francis Group

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

RSVP a temporal method for graphical authentication

Ashley A Cain & Jeremiah D Still

To cite this article: Ashley A Cain & Jeremiah D Still (2017): RSVP a temporal method for graphical authentication, Journal of Information Privacy and Security, DOI: 10.1080/15536548.2017.1397263

To link to this article: https://doi.org/10.1080/15536548.2017.1397263

Published online: 21 Nov 2017.

JOURNAL OF INFORMATION PRIVACY AND SECURITY
https://doi.org/10.1080/15536548.2017.1397263

RSVP a temporal method for graphical authentication

Ashley A Cain and Jeremiah D Still

Department of Psychology, Old Dominion University, Norfolk, VA, USA

ABSTRACT

We present a Rapid, Serial, Visual Presentation method (RSVP) for recognition-based graphical authentication. It presents a stream of rapid, degraded images, which makes the object recognition process difficult for casual attackers. Three studies investigated success rates for authenticating, RSVP's resistance to over-the-shoulder attacks (OSAs), approaches for facilitating learnability, and effects of resetting a passcode. We found that participants could successfully authenticate and could not complete OSAs. Learnability was promoted by the presentation of degraded versions of the images during the memorization phase. When a passcode was reset, participants successfully retrained themselves even when the previous passcode was recycled as distractors.

Introduction

Statement of the problem

Small touchscreen devices are used in public spaces and are increasingly providing access to sensitive data (e.g., email, contacts, and banking). There are many alternatives for authentication on these devices. However, we still lack authentication methods that are memorable, usable, and secure. Users need to be able to remember their password and successfully ignore old ones. They need to be able to authenticate quickly and easily without revealing their passcode to a nearby casual attacker. Few methods offer solutions for one touch while maintaining resistance to over-the-shoulder attacks (OSA).

Minimally, usable authentication methods need to make it difficult for casual onlookers to steal passwords in public places. They should not be able to easily perform OSAs or grease attacks (Dieter Findling & Mayrhofer, 2013), which occur when an attacker detects the traces left by fingers on a device's screen. Conventionally, new methods of authentication are evaluated by considering basic usability needs. For instance, being able to login in less than three attempts with a success rate of 80% or higher (Behl, Bhat, Ubhaykar, Godbole, & Kulkarni, 2014; Wiedenbeck, Waters, Sobrado, & Birget, 2006). However, new methods ought to empirically explore design decisions impacting practical implementation considerations (e.g., changing passcodes or training).

Alphanumeric (Nicholson, Coventry, & Briggs, 2013; Suo, Zhu, & Owen, 2005) and swipe passwords (Uellenbeck, Dürmuth, Wolf, & Holz, 2013) have been implemented and widely adopted. Alphanumeric passwords are problematic for memorability, which is a basic usability requirement for authentication methods (Still, Cain, & Schuster, 2017). Users must remember a series of numbers, symbols, and characters. For alphanumeric passwords to be secure, the string of characters must be long and use the full dimensional space (Eljetlawi & Ithnin, 2008). However, these long passwords are difficult to remember. Forgetting a password, or encoding a new one, is frustrating. Therefore users do not use the full dimensional space; rather they employ cognitive shortcuts. Creating a method that is more memorable by using pictures instead of a long, complex series of

CONTACT Ashley A Cain acain001@odu.edu; Jeremiah D Still jstill@odu.edu

characters helps users comply with better security practices. Memorability can be bolstered by graphical methods such as swipe passwords and others that leverage the picture superiority effect, which reflects richer encoding (Nelson, Reed, & Walling, 1976; Nickerson, 1965; Shepard, 1967; Standing, 1973; Standing, Conezio, & Haber, 1970). Pictures are encoded both visually, and semantically, so graphical passwords are more memorable due to this dual encoding (Paivio, 2013). For example, it is easier to remember a picture of Rebecca, a coworker in another division, than "! Rebecca1."

Alphanumeric passwords are also challenging to enter on a portable device. They require fine motor movements (Hayashi, Dhamija, Christin, & Perrig, 2008) and the use of multiple virtual keyboards (Schaub, Deyhle, & Weber, 2012). Small portable devices' authentication methods ought to be designed in a way that avoids the use of keyboards and dragging based interactions.

There has been extensive research showing graphical passwords provide better memorability and usability than alphanumeric passwords within the context of small touchscreens. For example, PassFace allows users to authenticate by selecting a picture of a face among distractor faces (RealUser). Evaluations of previous methods suggest they offer improvements for memorability and that there are still improvements yet to be made on security (Biddle, Chiasson, & Van Oorschot, 2012). Swipe passwords, a recall-based graphical method, have been widely implemented. Users authenticate using swipe by drawing a line through a series of dots on a grid. Swipe passwords are memorable and convenient on small touchscreens, but they do not meet the need for security. Swipe passwords are susceptible to over-the-shoulder attacks because the grid is clearly visible to onlookers (Cain, Chiu, Santiago, & Still, 2016). Previous research explains that these passwords are easy to observe and guess because users choose predictable patterns. Users tend to begin passwords in the upper left corner (Andriotis, Tryfonas, Oikonomou, & Yildiz, 2013), use three point lines (Uellenbeck et al., 2013), and end in the bottom right corner (Andriotis et al., 2013). These known cognitive shortcuts compromise security.

There is a need for better alternative methods of authentication for public use cases. Many graphical methods have been described in the literature (Bicakci, Atalay, Yuceel, Gurbaslar, & Erdeniz, 2009; Davis, Monrose, & Reiter, 2004; Hayashi et al., 2008; Pering, Sundar, Light, & Want, 2003; RealUser; Wiedenbeck et al., 2006). These methods offer greater memorability than alphanumeric passwords, and they tend to be easy to use with one touch (Davis et al., 2004; Hayashi et al., 2008; RealUser). However, the security of graphical methods has been criticized. Most methods present target passcodes statically and clearly visible within a grid. If these methods are visible to onlookers, they are not appropriate for securing valuable data. Some previous methods are designed to be resistant to over-the-shoulder attacks. For example, Use Your Illusion degrades images to confuse attackers (Hayashi et al., 2008). Convex Hull Click allows users to authenticate without directly clicking on the target passcode (Wiedenbeck et al., 2006). The assessment of the OSA vulnerabilities of any graphical passcode proposed is essential if the method is to be considered for more widespread use. Importantly, the practical implementation of graphical methods needs further investigation. A series of questions emerges. What are the best practices for learning a passcode? What happens when a user needs to reset a passcode; can the old passcode components be recycled into the database of distractors?

Existing graphical methods: Usability and resisting osas

Previous methods that are usable on a small screen tend to present target passcodes on a grid surrounded by distractors. Users need to move their attention spatially within the grids to select targets.

Recognition advantage

These previous graphical methods offer benefits for memorability. They leverage recognition over recall. Recognition-based graphical methods allow users to select their passcode from among

distractors. Recall-based methods require that users generate a passcode from memory. There are fewer stages of processing involved in recognition-based methods. Although both recognition and recall-based passwords leverage the picture superiority effect, these recognition-based graphical methods are particularly easy for users to remember over time. For example, Passface was found to be more memorable than alphanumeric passwords (Brostoff & Sasse, 2000). Passface (RealUser) is a method in which users' passcodes consist of three faces. Three subsequent 3 × 3 grids of faces are presented to users. Each target face is presented on each grid among distractor faces. Users select each of their three faces on three subsequent grids to authenticate. This method presents the target faces to the users, allowing them to recognize their targets rather than needing to generate their passcode from memory. Participants successfully logged in using Passface 11 out of 12 times after a ten month period, demonstrating its memorability. Passcodes in Passface are particularly memorable, not only because Passface is a recognition-based graphical method, but also because of humans' natural abilities for remembering faces. Passcodes for Story were also found to be memorable (Davis et al., 2004). Story is a method in which users' passcodes consist of images, such as a cup of coffee or a dolphin. Subsequent 3 × 3 grids of images are presented to users. Each target image is presented on each subsequent grid among distractor images. Users can recognize their passcode targets and authenticate by selecting each image on each subsequent grid. Users of Story are encouraged to tell themselves a story about each target as a mnemonic device to help remember images in their passcodes. Over 90% of participants remembered their passcodes for Story and successfully logged in after 80 days. Researchers also found that recognition-based passwords using icons allow for good memorability and low error rates (Wiedenbeck et al., 2006). Graphical Password with Icons (Bicakci et al., 2009) is a method in which users' passcodes consist of six icons. A 10 × 15 grid of icons is presented to users. The six target icons are presented on the grid among distractor icons. Users select their target icons on the grid to authenticate. The use of icons encourages users to have fewer biases in target selection. Convex Hull Click (Wiedenbeck et al., 2006) is a method in which users' passcodes consist of three or more icons. An interface containing an array of icons is presented to users. The three target icons are presented on the interface among distractor icons. Because there are at least three icons, the targets form a shape on the interface. Users authenticate by selecting any icon that in within the region created by their targets. By not clicking directly on an icon, this method offers resistance to OSAs. The Convex Hull Click recognition-based method using icons was found to be memorable. Fourteen out of 15 participants remembered their passcodes after one week.

Usable on small touchscreens

Typically, recognition-based methods allow users to authenticate with one touch. This quality makes recognition-based methods suitable for touchscreen devices so long as the targets can scale down well to small screens and the methods can offer fast, usable login durations. Passface (RealUser), Story (Davis et al., 2004), and Use Your Illusion (Hayashi et al., 2008), scale down well and allow for one-touch selection. The icon-based methods (Bicakci et al., 2009; Wiedenbeck et al., 2006) do not scale down well to small touchscreen devices. Although users can select targets with one touch on these previous methods, login times can be problematic because visual search might consume a consider amount of time. The user experience suffers when login durations are much longer than for alphanumeric passwords (Still et al., 2017). Previous research found that users can recognize faces in Passface with acceptable login durations comparable to alphanumeric passwords (Brostoff & Sasse, 2000). Graphical Password with Icons also offers login durations of around 12 seconds (Bicakci et al., 2009). Unfortunately, users needed around 71.66 seconds to log in using Convex Hull Click (Wiedenbeck et al., 2006), and they needed 27.7 seconds for Use your Illusion (Hayashi et al., 2008). Login durations are an important design hurdle to overcome.

OSA

The memorability of graphical methods and their login durations have been commonly examined. OSA vulnerabilities have caused concern, however. When targets are presented statically on a grid,

the targets may be particularly vulnerable. Passface (RealUser), Story (Davis et al., 2004), and Graphical Password with Icons (Bicakci et al., 2009) may put users at risk for observability, although the security of these methods regarding OSA has not been explicitly investigated. This concern was addressed by making the graphical passwords resistant to this type of attack. For example, Convex Hull Click (Wiedenbeck et al., 2006) was designed to protect passcodes from casual onlookers by allowing users to select anywhere inside the region created by their targets rather than directly selecting their targets.

Color Login (Gao, Liu, Dai, Wang, & Chang, 2009), Passmatrix (Sun, Chen, Yeh, & Cheng, 2016), Use Your Illusion (Hayashi et al., 2008), and a hybrid recognition and recall based approach (Zangooei, Mansoori, & Welch, 2012) were designed to be resistant to casual onlookers. Color Login presents images on a 9 × 9 grid. Users authenticate not by directly selecting their passcode images but by choosing the row they are in. It is unclear to attackers which image in the row is the target. Zangooei and colleagues' method presents images on a 4 × 4 grid. Passcodes consisted of four images. The grid of images disappears and is replaced by a grid of characters. Users can authenticate by typing the numbers associated with their images in a text box. It is hard for attackers to translate text that they observe to the associated images that are no longer on the screen. PassMatrix presents an image divided into cells. A passcode consists of one of the cells of the image. Across the top, there is a bar with a letter associated with each cell, and down the side, there is a bar with a letter linked to each cell. Users authenticate by scrolling to the correct cells using the bars on the top and side. Similar to Zangooei and colleagues' method, attackers of Passmarix would need to translate the text from the scroll bars to cells of the image. Passcodes for Use Your Illusion consist of three degraded images. Images are degraded by removing detail but retaining general colors and shapes. Three subsequent 3 × 3 grids of degraded images are presented to users. Each passcode target is presented on each subsequent grid among distractor images. To authenticate with Use Your Illusion, users recognize and select their targets. Each grid remains statically until the target is selected. It is theorized that degrading images interferes with attackers' object recognition, but it is possible for users who are already familiar with non-degraded targets to recognize their passcodes.

OSA performance was assessed for the methods described above. Participants took on the role of attacker. None identified the passcode for Color Login given one viewing of a login and three attempts to guess (Gao et al., 2009). Three out of ten participants identified the passcode for Zangooei and colleagues' (Zangooei et al., 2012) scheme given one viewing of a login. No participants identified the passcode for Passmartix based on screenshots from two logins (Sun et al., 2016). Cain, Werner, and Still (2017) reported that no participant was able to identify the passcode for Use Your Illusion after one viewing of a login, and nine out of 20 were able to determine the passcode given three viewings of logins. These graphical authentication methods (De Luca, Hertzschuch, & Hussmann, 2010; Liu, Gao, Wang, & Chang, 2011; Yamamoto, Kojima, & Nishigaki, 2009; Zakaria, Griffiths, Brostoff, & Yan, 2011) reflect approaches when executed appropriately offer security against onlookers, provide easy interactions, and boost memorability.

The RSVP method

We offer a rapid, serial visual presentation method (RSVP) that is suitable for small touchscreen devices used in public spaces. RSVP is novel among recognition-based methods, because target passcodes are presented temporally in rapid succession among distractors instead of within a spatial grid. A user's attention stays in one place while the images change. We used Snodgrass and Vanderwart's (1980) line drawings as targets and distractors. The passcodes were comprised of drawings of everyday objects that were selected by the system to avoid user biases. We degrade the line drawings to interfere with cognitive processes of object recognition by removing lines indicating curvature and intersections. See Figure 1 for examples of stimuli. According to Recognition-By-Components (RBC) theory, objects are recognized based on qualities of curvature, collinearity, symmetry, parallelism, and co-termination (Biederman, 1987). Degrading line drawings by removing key qualities needed for object recognition

Figure 1. Panel 'a' consists of whole line drawings that form a target passcode. In panel 'b' are the degraded versions of the targets that appear in the stream (Flickr; Good free photos; Pixaboy; Public domain pictures).

makes them only quickly recognizable if a user is familiar with the object (Biederman, 1987). Target selection is facilitated by implicit memory processes, specifically priming. Implicit memory allows participants to remember and respond to targets using unconscious memory processes (Schacter, Chiu, & Ochsner, 1993; Snodgrass & Corwin, 1988). Effects of priming for pictorial stimuli can occur after a single exposure to a stimulus, and priming effects for Snodgrass and Vanderwart's (1980) line drawing have been found to have be resilient, lasting six to 48 weeks (Cave, 1997). Previous research suggests that we can expect participants to have greater accuracy and response times to their target passcode that is primed (Cave, 1997), even for degraded versions of the stimuli (Snodgrass & Corwin, 1988). Target degraded images are presented in a random stream among seven distractor images, which are also degraded line drawings. A target image is never the first image in the stream to allow users to recognize the pace. See Figure 2 for an example of the stream.

Because of its rapid, serial component, this method leads to faster login durations than most previous, recognition-based graphical methods (i.e., 27–72 seconds; Hayashi et al., 2008; Pering et al., 2003; Wiedenbeck et al., 2006). The images flash on the screen in rapid succession. Each image is visible for 200 milliseconds and is separated by a one-second mask. The mask is a compilation of all of the images overlapping and functions to clear visual sensory memory. Users authenticated by hitting the space bar during each mask, because degraded object recognition takes one second (Biederman, 1987). Please note that login always takes 14 seconds.

While RSVP allows for shorter login durations, it retains advantages offered by previous methods of memorability and usability. This method is also usable with one touch. One image is on the screen at a time so that RSVP will scale down well to small touchscreen devices. To verify the feasibility of RSVP, study one examined rates of successful login.

RSVP method is designed to be resistant to OSAs because it is difficult for attackers to recognize a degraded line drawing, particularly at a rapid pace. We aimed to provide a method that will be suitable for securing sensitive data in public places. Study one also examines RSVP's resistance to OSAs to determine ability to maintain privacy in public spaces.

The next step for graphical methods is to investigate details of design decisions that impact usability following implementation. For example, there is a need for research about the process of resetting a passcode. There is a lack of knowledge about the effects of a previous passcode being

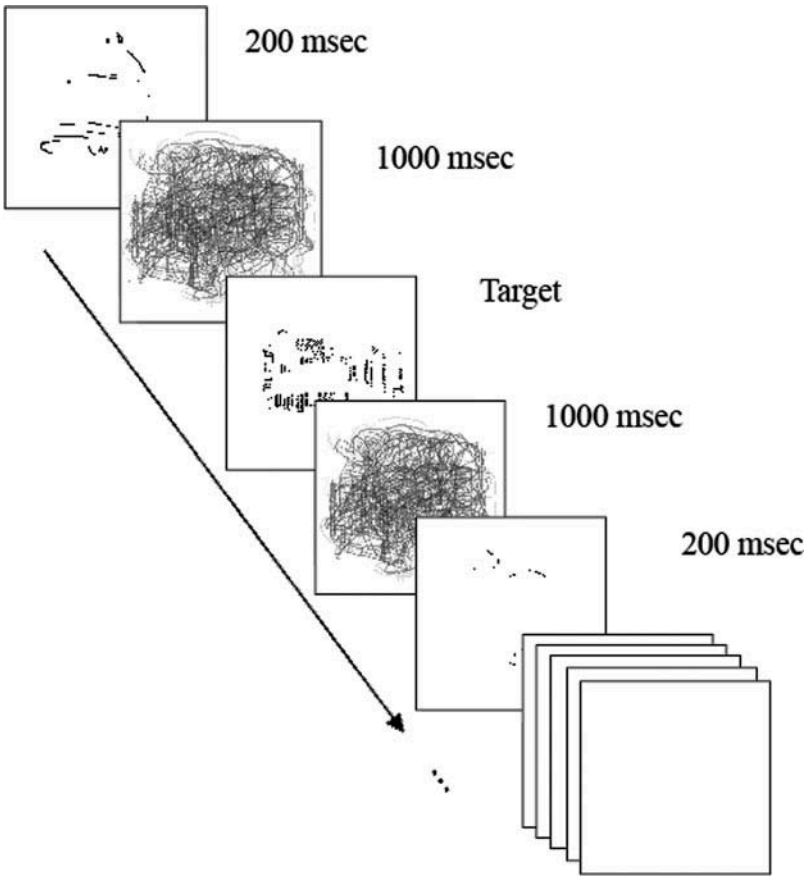

Figure 2. The stream was presented rapidly and serially. Targets and distractors flashed on the screen separated by masks. Participants selected targets using the space bar. Blank slides represent the continuation of the stream.

recycled as distractors. It may be difficult for users to log in successfully when a previous passcode becomes distractors. If users can quickly retrain themselves, the database of images would not need to be as extensive. There is also a lack of research about efficient ways to learn passcodes initially. For example, if images are degraded to protect against observability, there is a need for research about appropriate strategies to bolster learnability of degraded images. Users may be able to learn degraded versions of targets best when they are presented with the whole images during initial acquisition.

Study 1

In study one, we investigated participants' ability to authenticate using RSVP and its resistance to OSAs. We measured error rates for authentication attempts and their ability to recognize someone else's passcode.

Method

Participants

Ten undergraduate participants were recruited from the Introduction to Psychology course and were compensated with research credit.

Materials and procedure

Study one consisted of two parts. First, we observed participants' abilities to authenticate successfully. We measured error rates. Then participants viewed a video of a researcher authenticating. Participants took on the role of an attacker performing an OTS attack. We measured participants' abilities to identify passcode targets.

Ability to authenticate

Participants were greeted and provided with a consent form, which they read and signed. They were seated in front on a desktop computer where instructions and stimuli were presented in Paradigm©. They viewed a target passcode consisting of four whole Snodgrass and Vanderwart (1980) line drawings. Participants were instructed to memorize this passcode. Then the practice session began, consisting of ten authentication attempts. Degraded versions of the four targets flashed on the screen in a random, temporal order among seven distractors. When a degraded target flashed on the screen, participants hit the space bar. Participants were required to reach proficiency during the practice trials, or the practice trails would be redone. Proficiency constituted logging in successfully in at least the last three attempts in the practice trials. Typically, participants ran through the practice trials between one and three times. Practice trials were necessary to give the participants an opportunity to understand what they were expected to do to authenticate with RSVP. Then participants attempted to authenticate in ten experimental trials that resembled the practice trials. The targets were the same, and different distractors were used. Participants could make errors by either not hitting the space bar for their target or by hitting the space bar for a distractor. The experimental presentation software recorded errors.

OSA performance

Next, the experienced RSVP users took on the role of attackers. This allowed us to evaluate RSVP's resistance to OSAs. Participants viewed a video of a researcher authenticating using four degraded targets. When the researcher selected a target, there was the sound of a click. After viewing the video once, as an observer might in a public place, the participants were provided with a set of 260 non-degraded images. They were asked to identify the passcode they had observed. We recorded how many of the targets they were able to determine correctly.

Results

Number of attempts required for authentication

For the first part of study one, we found that participants could successfully authenticate using RSVP. All of the participants logged in at least once in three attempts. 84% of attempts to log in were successful overall (SD = 15.78). This success rate is similar to previous novel authentication methods (e.g., 80%; Behl et al., 2014; 86.67%; Sun et al., 2016; 90.35%; Wiedenbeck et al., 2006).

OSA performance

When participants took on the role of attackers, we found that none were able to observe the passcode. Half of the participants were able to identify only one in four targets. This finding suggests RSVP is resistant to casual OSAs.

Study 2

In study two, we compare presentations for the target passcode during the initial learning phase. It may be beneficial to present degraded images initially along with the whole target images because this may help prepare users to identify their degraded targets in the stream. Participants initially

Table 1. Percent Correct for learnability intervention.

Condition	*N*	*Percent correct*	*SD*
Whole line drawings presented alone	20	60.5%	1.61
Degraded versions presented	20	72.5%	2.27

viewed either degraded objects alone or with whole line drawings to determine the impact on learning.

Method

Participants

Twenty participants were recruited from the Introduction to Psychology course and were compensated with research credit. This was a different group of participants than in experiment one.

Procedure

After participants had reached proficiency in the practice session as they had in study one, participants authenticated ten times within each of the two experimental blocks. The blocks were counterbalanced to prevent order effects. Within one experimental block, participants viewed four whole line drawings and authenticated using the targets. In the other block, degraded versions were presented below each line drawing, and the participants authenticated using this new set of targets.

Results

We found that participants were able to successfully authenticate for the stimuli that was both presented with degraded versions and without them. In both conditions, 91.67% of attempts to authenticate were successful at least once in every three attempts. This finding verifies that participants can successfully log in using RSVP. Overall percentages correct indicate that there was a benefit for learnability for presenting degraded line drawings with the whole images (see Table 1). 72.5% (SD = 2.27) of authentication attempts were successful when the degraded versions were initially presented, which shows an improvement compared with the 60.5% (SD = 1.61) success rate for the whole line drawings presented alone, $t(19) = 2.42$, $p = .03$, $d = .54$. Improvements for learnability with degraded line drawings are also suggested by a numerically higher success rate for the first three attempts. For the degraded stimuli condition, 85% of participants successfully logged in in their first three attempts. 80% of participants logged in in these early attempts in non-degraded stimuli condition.

Study 3

In study three, we explored the effects of changing a passcode. Practically, it may be useful to recycle old passcodes back into the database. However, there is a possibility that the previous passcode would cause false alarms when it becomes a distractor. Participants learned a new passcode in the second experimental block of trials. Now the first block's targets appear as distractors in half of the trails. These findings will empirically support the decision to either retire passcodes or reuse them in the database.

Method

Participants

Twenty-three undergraduate participants were recruited from the Introduction to Psychology course and were compensated with research credit. Again, new participants were recruited.

Table 2. Success rates for recycling previous passcode.

Condition	*N*	*Success Rate*	*SD*
Previous passcode became distractors	20	8.43	1.16
Previous passcode was not distractors	20	8.43	0.84

Procedure

As in study one and two, participants performed a practice session until they reached proficiency. Throughout this study, target images were initially presented with their degraded versions. After the first practice session, each participant logged in ten times in an experimental block using the same targets as the practice block. Then participants performed a second practice block. They practiced ten logins. Next, participants logged in 20 times using new targets in an experimental block. Ten trials contained the previous password as distractors and ten did not. These trials were presented in a pseudorandom order.

Results

A paired sample T-test revealed that participants performed better in the first experimental block than the second block. In the first block, participants made fewer errors (M = 9.17 correct inputs in each authentication attempt, SD = 0.94) than in block second (M = 8.43, SD = 0.84), $t(22)$ = 3.36, $p < .01$. These results suggest that participants had more difficulty authenticating in the second block, because, although they had two practice sessions, they did not practice the new password until they reached proficiency as they had in the first block. We used a paired samples T-test to compare performance differences between trials in the second block in which the previous passcode became distractors and those in which it did not (see Table 2). We found that there was no difference for rates of successful authentication when the previous passcode became distractors (M = 8.43, SD = 1.16) or did not (M = 8.43, SD = 0.84), $t(22)$ = 0.00, $p > .05$. For the trials that had the old passcode as distractors, we compared error rates for clicking on the old passcode versus other distractors. It appears that old passcode performance numerically decreased (97% correct) by only 2% compared with not having familiar distractors (99% correct) in the stream.

Discussion

Across three studies we explored rates of successful login for RSVP, its resistance to OSAs, effective techniques for learnability, and impacts of reusing old passcodes as distractors. We found that participants could authenticate effectively and that this method is resistant to casual onlookers. We suspected during the practice session in study one that performance increased when participants became familiar with degraded versions of images. In study two, we found that passwords are most effectively learned when degraded versions of line drawings are presented with whole images during the initial learning phase. In study three we examine the impact of reusing an old passcode as distractors. When a user needs to use a new password, there is little impact of the previous password becoming distractors. Even though users identify targets quickly as they appear to jump out in the stream, participants were able to inhibit the selection of their previous passcode. We suspect that participants engaged with the old passcode as it flashed on the screen, but the time allowed for a response was robust enough to enable participants to inhibit their response efficiently and respond to the new targets (except for, 2% slip errors). If old and new targets appeared within a temporal window of 250 to 500 milliseconds of each other, it is likely that an old target would harm the identification of the new target, commonly referred to as an attentional blink (Potter, Chun, Banks, & Muckenhoupt, 1998). The longer response window of our mask likely allowed for fewer false

alarms for old targets and misses for new targets. Results from study three suggest that previous passcodes do not need to be retired from the database.

RSVP method builds on previous methods that have been memorable and usable with one touch (Davis et al., 2004; RealUser). It adopts a method of degrading images from Use Your Illusion (Hayashi et al., 2008). Differently, than Use Your Illusion, images are presented temporally rather than spatially. Authors of Use Your Illusion theorized that degrading images would make them resistant to the OSAs. However, this assumption was not experimentally verified. The current study verifies that the degraded images used in RSVP are not recognizable to attackers and are only identifiable to users who are already familiar with the passcode. Degrading line drawing by removing lines for curvature and intersection provided resistance to OSAs.

The largest contribution made by RSVP is the temporal component. When images are presented one at a time in a rapid stream, login durations are constrained by the system to be 14 seconds. This allows RSVP to have faster login durations than most previous graphical methods (RealUser; Wiedenbeck et al., 2006). Fast login durations not only improve user satisfaction, but they also function to bolster security further. OSAs are harder to complete when target images are on the screen only briefly. Also, authenticating with one touch protects passcodes from finger grease attacks, as users tap the screen instead of drawing a line. A rapid, serial method adds these components of speed and security while retaining advancements made by graphical methods for memorability and usability.

Conclusion

RSVP offers an authentication method that retains the advantages of previous recognition-based graphical methods, and it overcomes some previous shortcomings such as login durations and observability. This method is usable with one touch. It ought to scale down well to small touchscreen devices because one image is presented at a time. However, the real-world suitability of RSVP's for small touchscreens needs to be explored in future research.

Uniquely, this method is rapid and serial, which makes images harder to observe. Security of RSVP is further bolstered by the use of degraded images. Making object recognition more difficult by removing lines from curvature and intersections prevents a causal attacker who is unfamiliar with the passcode.

No participants could successfully observe the passcode when they took on the role of attackers. The current research also demonstrates that users would be able to successfully login using this method. Furthermore, details of implementation have been explored. When a user is learning a new passcode, the degraded line drawings should be presented with the whole line drawings. When a user needs to reset their passcode, the previous passcode can be recycled in the database. It does not interfere with the new passcode when the previous passcode becomes distractors. This novel, temporal method for authentication provides a fast, easy, secure, and implementable way to secure data. It is particularly suitable and meets a need for securing sensitive data on small touchscreen devices. Future work should investigate RSVP's resistance to other types of attacks, such as intersection attacks. It should also investigate user acceptance of RSVP for securing specific applications on touchscreen devices and the device in general.

Notes on contributors

Ashley Cain is a Human Factors PhD student at Old Dominion University, where her research focuses on the human side of cyber security, specifically authentication. She completed her master's degree at San Jose State University where she also studied human factors and cyber security.

Jeremiah Still earned his Ph.D. in Human-Computer Interaction from Iowa State University. He is an Assistant Professor of Psychology at Old Dominion University. His Psychology of Design (PoD) laboratory explores the relationship between human cognition and technology; specifically, he is focusing on: visual attention, usable cybersecurity, and intuitive design.

References

Andriotis, P., Tryfonas, T., Oikonomou, G., & Yildiz, C. (2013). A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Budapest, Hungary; 1–6.

Behl, U., Bhat, D., Ubhaykar, N., Godbole, V., & Kulkarni, S. (2014). Multi-level scalable textual-graphical password authentication scheme for web based applications. *REV Journal on Electronics and Communications*, *3*(3–4), 116–123. doi:10.21553/rev-jec.64

Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H., & Erdeniz, B. (2009). Towards usable solutions to graphical password hotspot problem. *In 33rd Annual IEEE International Conference of Computer Software and Applications Conference*, *2*, 318–323.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 19. doi:10.1145/2333112.2333114

Biederman, I. (1987). Recognition-by-components: A theory of human image understanding. *Psychological Review*, *94* (2), 115–147. doi:10.1037/0033-295X.94.2.115

Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation. In McDonald, S., et al. (Eds.) *People and computers XIV—Usability or else!* (pp. 405–424). Berlin, London : Springer.

Cain, A. A., Chiu, L., Santiago, F., & Still, J. D. (2016). Swipe authentication: Exploring over-the-shoulder-attack performance. Proceedings of the *7th International Conference on Applied Human Factors and Ergonomics (AHFE 2016)*. Orlando, FL.

Cain, A. A., Werner, S., & Still, J. D. (2017). Graphical authentication resistance to over-the-shoulder-attacks. *Proceeding of CHI in Late-Breaking Work*. Montréal, Canada.

Cave, C. B. (1997). Very long-lasting priming in picture naming. *Psychological Science*, *8*(4), 322–325. doi:10.1111/j.1467-9280.1997.tb00446.x

Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. Proceedings of the 13th USENIX Security Symposium, San Diego (Vol. 13, pp. 11–11).

De Luca, A., Hertzschuch, K., & Hussmann, H. (2010). ColorPIN: Securing PIN entry through indirect input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, GA, 1103–1106.

Dieter Findling, R., & Mayrhofer, R. (2013). Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices. *International Journal of Pervasive Computing and Communications*, *9*(3), 190–208. doi:10.1108/IJPCC-05-2013-0012

Eljetlawi, A. M., & Ithnin, N. (2008). Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. *In Third International Conference of Convergence and Hybrid Information Technology*, *2*, 1137–1143. Flickr. Retrieved October, 2017 from https://www.flickr.com/photos/playingwithpsp/278491699

Gao, H., Liu, X., Dai, R., Wang, S., & Chang, X. (2009). Analysis and evaluation of the colorlogin graphical password scheme. In *Fifth International Conference on Image and Graphics*, Xi'an, Shanxi, China, 722–727.

Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: Secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, Pittsburgh, PA, 35–45. Good free photos. Retrieved October, 2017 from https://www.goodfreephotos.com/vector-images/goblet-line-drawingvector-clipart.png.php

Liu, X. Y., Gao, H. C., Wang, L. M., & Chang, X. L. (2011). An enhanced drawing reproduction graphical password strategy. *Journal of Computer Science and Technology*, *26*(6), 988–999. doi:10.1007/s11390-011-1195-7

Nelson, D. L., Reed, V. S., & Walling, J. R. (1976). Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, *2*(5), 523.

Nicholson, J., Coventry, L., & Briggs, P. (2013). Faces and Pictures: Understanding age differences in two types of graphical authentications. *International Journal of Human-Computer Studies*, *71*(10), 958–966. doi:10.1016/j.ijhcs.2013.07.001

Nickerson, R. S. (1965). Short-term memory for complex meaningful visual configurations: A demonstration of capacity. *Canadian Journal of Psychology/Revue Canadienne De Psychologie*, Erlbaum, *19*(2), 155–160. doi:10.1037/h0082899

Paivio, A. (2013). *Imagery and verbal processes*. Psychology Press.

Pering, T., Sundar, M., Light, J., & Want, R. (2003). Photographic authentication through untrusted terminals. *IEEE Pervasive Computing*, *2*(1), 30–36. doi:10.1109/MPRV.2003.1186723

Potter, M. C., Chun, M. M., Banks, B. S., & Muckenhoupt, M. (1998). Two attentional deficits in serial target search: The visual attentional blink and an amodal task-switch deficit. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *24*(4), 979. Public domain pictures. Retrieved October, 2017 from http://www.publicdomainpictures.net/view-image.php?image=184516&picture=kitten-lineart-drawing

RealUser. Retrieved June, 2005 from www.realuser.com.

Schacter, D. L., Chiu, C. Y. P., & Ochsner, K. N. (1993). Implicit memory: A selective review. *Annual Review of Neuroscience*, *16*(1), 159–182. doi:10.1146/annurev.ne.16.030193.001111

Schaub, F., Deyhle, R., & Weber, M. (2012). Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, New York, NY, 13–23.

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior*, *6*(1), 156–163. doi:10.1016/S0022-5371(67)80067-7

Snodgrass, J. G., & Corwin, J. (1988). Perceptual identification thresholds for 150 fragmented pictures from the Snodgrass and Vanderwart picture set. *Perceptual and Motor Skills*, *67*(1), 3–36. doi:10.2466/pms.1988.67.1.3

Snodgrass, J. G., & Vanderwart, M. (1980). A standardized set of 260 pictures: Norms for name agreement, image agreement, familiarity, and visual complexity. *Journal of Experimental Psychology: Human Learning and Memory*, *6* (2), 174.

Standing, L. (1973). Learning 10000 pictures. *The Quarterly Journal of Experimental Psychology*, *25*(2), 207–222. doi:10.1080/14640747308400340

Standing, L., Conezio, J., & Haber, R. N. (1970). Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science*, *19*(2), 73–74. doi:10.3758/BF03337426

Still, J. D., Cain, A. A., & Schuster, D. (2017). Human-centered authentication guidelines. *Journal of Information and Computer Security*.

Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2016). A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing, 99:* 1–14.

Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical passwords: A survey. In *Computer Security Applications Conference, 21st Annual*, Tucson, AZ, 463–472.

Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. (2013). Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, Berlin, Germany, 161–172.

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the Working Conference on Advanced Visual Interfaces*, New York, NY, 177–184.

Yamamoto, T., Kojima, Y., & Nishigaki, M. (2009). A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection. In *Security and Management*, Las Vegas, Nevada, 188–194.

Zakaria, N. H., Griffiths, D., Brostoff, S., & Yan, J. (2011). Shoulder surfing defense for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, New York, NY, 6–18.

Zangooei, T., Mansoori, M., & Welch, I. (2012). A hybrid recognition and recall based approach in graphical passwords. In *Proceedings of the 24th Australian Computer-Human Interaction Conference*, Melbourne, VIC, Australia, 665–673.