TAPI: Touch-screen Authentication using Partitioned Images

Jonathan Citty, Dugald Ralph Hutchings
Computing Sciences Department, College of Arts and Sciences

***Abstract*—We describe and evaluate an alternative approach to a personal identification number (PIN) for small touch-screen devices named *TAPI*. TAPI replaces a 4-digit sequence with a sequence of 4 partitions of a selection of 16 images, increasing the possible combination of authentication sequences from 10^5 to over 10^7 but decreasing the screen space allocated to each possible selection. Across two user studies of TAPI in which 30 participants were randomly assigned authentication sequences, 90% of participants were able to both remember and enter their authentication sequence after one week of non-use. Median sequence entry times were 4.6 seconds on a higher-resolution touch-screen device and 7.1 seconds on a lower-resolution device. Participants generally indicated that they were satisfied with the interaction and would consider adopting TAPI for everyday use. Design and other considerations are also discussed.**

***Index Terms*—computer security, user interface human factors**

I. Introduction

Use of mobile devices to accomplish everyday computing tasks appears to be becoming a commonplace activity. For example, the Pew Research Center reported in July 2009, "56% of adult Americans have accessed the internet by wireless means, such as using a laptop, mobile device, game console, or MP3 player," and "one-third of Americans (32%) have used a cell phone or Smartphone to access the Internet for emailing, instant-messaging, or information-seeking" [11]. Phones and other devices designed for Web use and access are increasingly relying upon touch-screens to allow users additional methods of interaction, including graphical interaction (such as GUI button clicking) and a soft (on-screen) keyboard.

To protect the applications and data stored on mobile devices, a prevailing method is the entry of a personal identification number (PIN) for authentication; users must enter a previously created 4-digit sequence to begin using the device. On small touch-screen devices, PINs have a natural speed-of-entry advantage over textual character sequences (which in this paper we call *passwords*) because with PINs, the screen space needs to be divided among only ten options (numbers 0 through 9) whereas with text, the screen needs to be divided among many more options (26, 40, or more). Given larger targets, users are considerably less likely to make tapping errors. PINs of course are also easier to remember than typical 6- or 8-character passwords (which often have additional constraints such as "must contain a non-alphanumeric character.") The tradeoff that users make in using the fast-to-enter and easy-to-remember PIN system is a significant loss of security because a third party intent on gaining unauthorized access to the user's device can more easily guess the authentication sequence (and perhaps more easily determine the PIN through social engineering). Unfortunately, as mobile devices increasingly can be used to accomplish everyday tasks, such easily attacked authentication mechanisms become unsuitable or undesirable. We thus have the so-called *password problem*: authentication sequences should be easy to use (by quick recall and entry) but difficult to guess or attack [15]. Given the increased difficulty of selecting textual characters on a touch screen device, speed of entry is particularly important on this platform.

Our work addresses the password problem for mobile touch-screen devices. We propose the Touch-screen Authentication using Partitioned Images (TAPI) system to provide authentication sequences that exhibit high memorability while increasing

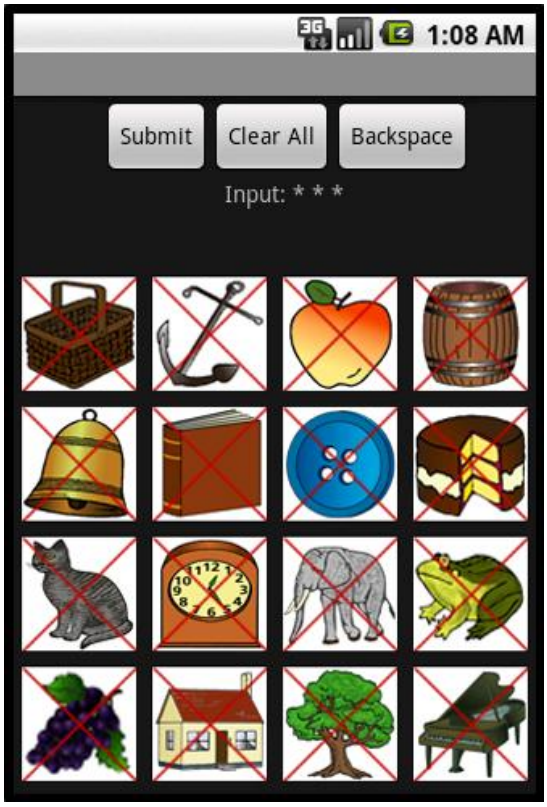

Fig. 1: The TAPI entry system in which the user has already tapped three image partitions of the four-image authentication sequence.

the number of possible sequences, making attack through guessing less likely to succeed. The user's authentication sequence consists of partitioned images rather than numbers but otherwise works in the same manner as a PIN system (Fig. 1). In short, TAPI increases security by having the user not only enter one of 16 images image in proper sequence, but also to select a correct partition of the image (in Fig. 1, the partitions of each image are top, right, bottom, and left as marked by the red Xs). Users are thus selecting from 64 possible options at a time rather than ten options, like most PIN systems. We address memorability, speed of entry, and user satisfaction by presenting and analyzing the results of two user studies of TAPI on two types of handheld touch-screen devices. First however we address how TAPI relates to other research.

II. Related Work

At SAM 2004, Jansen et al. presented a framework for mobile device security which included a method of allowing a variety of "password user interfaces" to be used in a flexible way [9], including a graphical method proposed by Jansen et al. in earlier work [8]. Jansen provides evidence of the feasibility of a graphical approach and focused on the variety of reasons for adopting the approach, but did not include a user study. As a result in our work, we omit details on the technical feasibility of the approach but instead focus on the results of a user study of a particular image sequence system (TAPI) on a prevailing input hardware platform (touch-screen devices). Jansen also provides an excellent overview of a variety of early commercial systems (but as with Jansen's system, to our knowledge, none have been examined with a user study and further, none adopt the partitioned image approach).

TAPI is most directly influenced by the work of Komanduri and Hutchings (KH), who compared standard text-based passwords to a complementary image-based approach in which participants selected a sequence of images to authenticate [10]. In a user study, twice as many image-based participants could accurately recall and enter their image sequence (as compared password participants) after a week on non-use (and interestingly, the remaining participants remembered all of the images in their sequence but entered the images out of sequence). KH carefully selected the images from which users chose to exploit the *picture superiority effect*, which in essence indicates that images are more memorable than text [4], as long as the set of images being remembered are not similar to one another [12]. TAPI uses a subset of the images of the KH system that each are easy to identify even when scaled down to a smaller pixel space and partitions each image to create more possible points of selection in a limited screen space without needing to scroll or zoom to interact.

The notion of differentiating portions of an image to provide additional possible selection points arises in Wiedenbeck's et al. series of papers describing and analyzing the PassPoints system (e.g., [16]). In PassPoints, users choose a number of regions of a large image and subsequently click those regions in sequence in order to authenticate. Results of studies of PassPoints have generally been positive (e.g., [17]), but we are unaware of any studies of the usability of the system on small touch-screens. Further, in the studies of PassPoints users were allowed to select their own image point sequences whereas in the KH work, the image sequence was randomly generated and then assigned to the user. Motivation for this decision comes from observations that PassPoints users tend to select prominent image features [14], thus yielding image point sequences that are easier to attack through guessing.

Our work is further motivated by the results from Brostoff and Sasse concerning PassFaces [1], a graphical authentication system intended to replace a PIN approach. In PassFaces, the users are presented with a grid of 9 distinct human faces four consecutive times and in each grid, must select the correct face that is part of the authentication sequence. While memorability was found to be high, the time required to authenticate was not reported by the authors. Users however responded in subjective feedback that they felt that the method required too much time. Further, the system was not assessed in a small-screen or touch-screen environment, but rather on standard desktop personal computers. The authors called for graphical authentication systems with reasonable sequence entry times.

PINs have also been directly compared to image sequences, but unlike the way that we propose in this paper. For example, Dhajima and Perrig [5] found that participants in a user study of whole images relative to PINs, users were able to remember image sequences more easily but required too much time to authenticate (approximately thirty seconds, well above the results we will report). De Angeli et al. [3] proposed VIP in response and assigned participants an image sequence from a grid of ten or sixteen possible choices, finding high memorability and reasonable speed-of-entry results (there were three VIP variations and the best approach exhibited mean entry time of approximately seven seconds). We look to examine whether partitioned images can provide reasonable speed of entry, thereby increasing the security since more selections are possible at each point in the sequence entry. Further, while VIP was evaluated in a touch-screen environment, it does not appear to have been evaluated on a small screen such as those found on mobile devices.

Awase-E on the other hand is a graphical authentication system designed specifically for a mobile phone (i.e., a small-screen device) [13]. In this system, users select an authentication sequence consisting of photographs from their personal collection which are then interspersed with a collection of other "standard" images. We find two significant limitations with this approach: (1) there is an assumption that users have photographs at all on their personal device and (2) even if users do have such photographs, an attacker might be able to easily guess which photographs belong to a user because they are visually quite different from the standard set. We examine user performance when the authentication sequence is randomly assigned. As with other graphical approaches, Awase-E user authentication sequences exhibited high memorability in a user study. The authors did not report user performance times

however.

In summary, image sequence authentication methods often exhibit high memorability but undesirably high entry times. VIP is a notable exception, but VIP was not tested with small screens where image visibility and small target size might be an issue. Our design and subsequent evaluation of TAPI addresses these observations.

III. TAPI System Design Considerations

Our initial exploration of TAPI began with the question of whether the KH system [10], which used a 10-image by 8-image grid, could be adapted to operate in a usable fashion on small-screen devices. As a result, we began design by selecting images used in the KH system that could be scaled to smaller pixel sizes yet still be easily perceived. Our personal observations using the T-Mobile G1 device led us to the 4-image by 4-image layout depicted in Fig. 1. We then informally experimented with different partition sizes and users possessing different finger girths, finding that most users could reliably select images containing 4 equally-sized partitions after a brief practice session. We chose the X-shaped partition lines by appealing to the picture superiority effect: the regions could be remembered physically or by textual labels (such as top, right, left, bottom; or north, east, south, west). Furthermore, the locations of the images would be fixed (just as keyboard character locations do not change for password entry) to allow sequences to be remembered by the pictures they contained and by the location of those pictures. In the future work section we discuss different partition and layout strategies that could also be adopted.

Next in our design process we discussed the visual presentation of user interaction. For example in a typical password entry scenario, the user sees an on-screen dot representing each character entered in the password. This allows the user some feedback to confirm that a key was pressed, but disallows a casual observer from seeing the entered text. We adopted this approach (as did KH, though they also supported users entering image sequences via keyboard equivalents). Some modern mobile devices offer further feedback. For example, in *password entry* (not PIN entry) the Apple iTouch and iPhone devices show an enlarged version of the on-screen keyboard key each time the user taps the key in addition to showing the key character in clear text for approximately 500ms to allow the user to confirm what was entered. Given that we are trying to improve the overall security of authentication sequence entry, we decided to provide no further feedback of the image partition that was actually selected by the user. Note too that the picture superiority effect applies to all people: not only can the user remember images more easily than text, but so too can a malicious observer trying to steal a user's authentication sequence. Partitions help to keep TAPI resistant (but not immune) to "shoulder surfing" since an observer may be able to see what image was selected but will likely be less accurate in observing which specific partition was selected, depending on the viewing angle of the observer.

Fig. 2: Feedback provided during the TAPI training session. As the user taps on the image partitions, the user sees a textual description of the tap (image name and partition location). The numbers below the text allow the examiner to track the progress of the participant. 0/0/1 means that the participant has entered 0 correct sequences consecutively, 0 correct sequences overall, and 1 incorrect sequence.

IV. Initial User Study

A. Methods

We recruited students from our university to participate in a user study of TAPI. Fifteen participants (two female, thirteen male) between the ages of 18 and 23 enrolled. All participants were at least weekly users of mobile devices and thirteen participants used a touch screen at least once weekly. Each participant began the study by arriving in our lab. After completing the informed consent process, the experimenter provided a brief overview of the TAPI system and allowed the participant to ask any questions about TAPI.

Participants then received a pre-assembled "authentication sequence book," a series of four pages, each of which has the appearance of Fig. 1 except each page p highlights the p^{th} section of an image in the participant's authentication sequence. The participant was given up to five minutes to interact with the book (one participant used all five minutes but all others used two minutes or less). Participants then returned the book to the experimenter and received a demographic survey to complete. The experimenter ensured that a minimum of five minutes passed between the time the participant received the book and the time that the participant proceeded to the next step of entering the authentication sequence on a T-Mobile G1 device (screen size: 47mm wide by 71mm high; resolution: 320 pixels wide by 480 pixels high). Each image was 72 pixels square, yielding 4 triangular partitions with a base of 72 pixels and a height of 36 pixels (approximately 10.6mm and 5.3mm respectively).

Training proceeded with the participant entering his or her authentication sequence and clicking *Submit*. As the participant entered the sequence, clear text feedback was provided to inform the participant which image and which partition was tapped (Fig. 2). The participant was informed whether the entry was successful or unsuccessful. The process repeats until the participant reaches one of the following conditions:

- the correct authentication sequence has been entered correctly five *consecutive* times (at which point the participant continues onto the next phase); or
- an incorrect authentication sequence has been entered five *total* times (at which point the participant receives the book, re-examines it, and re-starts the training phase; 3

TABLE I
USER SEQUENCE ENTRY TIMES (MEASURED IN SECONDS)
INITIAL STUDY USING T-MOBILE G1 DEVICE

Phase Description	Incorrect Submission	Mean	Median
Training	included	13.2	12.9
Confirmation	included	42.3	19.7
Final	included	44.4	17.7
Training	excluded	11.5	11.0
Confirmation	excluded	10.9	10.4
Final	excluded	8.6	7.1

TABLE II
USER SEQUENCE ENTRY TIMES (MEASURED IN SECONDS)
FOLLOW-UP STUDY USING VERIZON DROID DEVICE

Phase Description	Incorrect Submission	Mean	Median
Training	included	8.3	6.8
Confirmation	included	12.1	8.1
Final	included	12.1	8.2
Training	excluded	7.5	6.8
Confirmation	excluded	6.9	5.5
Final	excluded	5.6	4.6

participants needed to return to training and each returned only once).

Participants then completed a survey of their impressions of TAPI. Afterward, participants entered the *confirmation* phase of the experiment by correctly entering the authentication sequence one time without cleartext feedback (all participants were able to do this in three attempts or less). Instead, a dot appeared each time that participant selected any image area, as seen in Fig. 1. The experimenter then asked the participant not to write down the authentication sequence and left the lab. One week later, participants returned to the lab for the *final* phase of the experiment. Participants re-entered the authentication sequence and received only the dot feedback as they touched the image areas. If a participant entered an incorrect sequence, then the participant tried to enter the sequence again. This repetition continued until the participant either entered the correct sequence or claimed that he or she could not successfully enter the sequence. Following this *final* phase, the participant completed a survey of their opinion of TAPI. Each participant received $5 for participating.

At all times during interaction on the device, our experimentation software recorded participant interaction with a timestamp accurate to 1ms. The following objective analysis is of the data collected and reported by the software. The reader should note that in an actual implementation of TAPI, participants would not receive their training on paper but would instead engage in the training entirely on the device itself.

B. Results

Of the fifteen participants, fourteen correctly entered the authentication sequence in the final phase (93%). The other participant remembered the correct images and partitions, but transposed two of the partitions in the sequence (this is consistent with the KH results [10]).

Although TAPI provides a larger authentication sequence space than a PIN system and also provides high memorability, user entry times were longer than might be desirable but consistent with the performance of VIP [3], as indicated in the related work section. The determination of an entry time is somewhat more complicated than at first glance. Various events can transpire between the first tap that a user makes and the final tap of the submit button. The user might hit the *backspace* or *clear all* buttons, which respectively remove the most recent tap or all previous taps. The user might also first enter an incorrect sequence, then try again and enter a correct sequence. An argument could be made to include or exclude "erroneous" actions. Our preference is for conservative but accurate estimation, so in Table I we separately report times that *include* and *exclude* incorrect sequences and in both cases, include the time used to tap backspace or clear all buttons. We also report the mean and median times since participants were encouraged to keep trying to enter the sequence until they were correct, even in case when the participant was fairly confident that he or she had forgotten the sequence. When this occurs, the participant exhibits a sequence entry time that is well above the average and skews the results.

It is somewhat surprising that when excluding incorrect submissions, the median entry time decreases as the participant moves from phase to phase. In training, the participant receives clear text feedback about their entry and practices the entry sequence several times. In confirmation, the participant enters the sequence only once and without clear text feedback. In the final phase, the participant has not used TAPI for a week. If we examine the fastest entry sequence of each participant in the training phase, we find a median entry time of 6.0s. It seems that over time, users are able to approach their fastest practiced entry time even without practice.

Nevertheless, it is questionable whether 6.0s or 7.1s is fast enough for a 4-item sequence, even though it is comparable to VIP [3]. This is a reasonably short period of time, but PIN entry is likely much faster due to larger target sizes and a smaller possible set of sequences (in VIP, the PIN entry was faster than any graphical method [3]). We propose however that TAPI entry times are fairly short and not overly burdensome and may well be worth the extra security provided to the user (and to the organization that owns the device in situations where the device is a work-related item and not primarily a personal item). We observed during the experiments that almost all non-sequence errors that users made were a result of accidentally tapping a neighboring partition. To understand whether we could allow for faster entry, we re-ran the experiment on a device with a more sensitive touch surface and higher screen resolution. We discuss the results of that study momentarily.

Despite the somewhat slow times, users were generally positive about the interaction with the system, with eleven of fifteen participants indicating overall satisfaction (and the remaining four all commenting that the partition areas were too small to reliably tap). Of the fourteen participants who remembered their image sequences, only two indicated that they had difficulty remembering the sequence but twelve indicated

that they experienced some difficulties in entering the sequence because of difficulty in actually tapping the correct area despite knowing (and seeing) where to tap. This analysis further prompted us to re-evaluate the system on a slightly larger screen with a finer-grained resolution. Finally, it is interesting to note that when participants were asked to transcribe their sequences, twelve of fourteen listed the partition location first, then the image name, even though in training the opposite presentation was used in the feedback area. This suggests that in a formal implementation, the feedback should be changed to better match how participants actually remember their sequences.

V. Follow-up User Study

A. Methods

We conducted the same experiment as described above except for the following changes:

- the actual participants were different people (14 males, 1 female, all between 18 and 23 years in age, and all touch-screen mobile device users on at least a weekly basis);
- the hardware was a Verizon Droid (screen size: 48mm wide by 86mm high; resolution: 480 pixels wide by 854 pixels high); and
- we asked the participants to enter their authentication sequence multiple times in the *final* phase in order to better assess practiced entry time rather than only "cold start" entry time after a long period of non-use.

With the increase in screen size and resolution, the target size also increased. Each image was 118 pixels square, creating triangular partitions with a height of 59 pixels (approximately 11.6mm and 5.8mm respectively, an increase of about 1mm and 0.5mm compared to the G1 device).

B. Results

Of the fifteen participants, thirteen correctly entered the authentication sequence in the final phase (87%). Both mean and median entry times improved considerably, as displayed in Table II. The median entry time to enter the correct sequence, excluding incorrect attempts, dropped from 7.1s in the initial study to 4.6s in the follow-up study. Further, we analyzed the data to uncover the median fastest entry time in both the training and the final phases, finding respective times of 3.9s and 3.5s (compared to 6.0s from the initial study). We would expect that as users become more practiced in entering their TAPI sequence, their performance would tend toward these fastest median times. Interestingly in the VIP study, which took place on a much larger touch-screen, PIN performance was also about 3.5s [3].

Of the thirteen participants who remembered their sequences, eight indicated that they had no difficulty recalling their sequence and four indicated that once they examined the picture grid, they were able to recall the sequence (the remaining participant had more difficulty). Four of thirteen participants indicated that they experienced difficulty in entering the sequence. Eleven of thirteen participants rated the system as positive overall, one participant rated the system as negative because his large fingers make touch-screen interaction generally difficult, and one participant was neutral.

VI. Discussion

Our results indicate that TAPI can provide users with reasonably high memorability and reasonably short entry times. As compared to PIN systems, the entry time is likely a bit slower but exhibits higher overall security. An open research question is what the desirable balance of security and efficiency is for individual users and for organizations. There are several ways in which TAPI could be further modified to provide improvements in either of these categories. Using more images or more partitions increases security by providing more options, but decreases target size and thus increases the chance for error and likely the time needed for correct sequence entry. Zooming and scrolling could be considered, but would almost certainly significantly increase entry times. Adjusting the location of the images in the grid would help the system become more resistant to shoulder surfing (because now screen location is not a clue to revealing the image sequence) but might hamper memorability. Providing brief visual feedback to the participant would help to eliminate tapping errors, but also decreases security by allowing a casual observer a better chance to steal the sequence. Partitioning images based on the images themselves rather than a uniform area might improve memorability to 100% (for example, a cat might be separated into partitions of head, paws, belly, and tail). If the touch-screen allows the user to touch multiple screen areas simultaneously (often called "multi-touch"), pairs of images or image partitions could comprise the authentication sequence.

Another aspect of time in this work is whether users are willing to be assigned random image sequences and take two minutes to practice entering the sequence. Perhaps this is unlikely with personal mobile devices, but organizations might be able to enforce such policies. Although it is true that average entry time should also consider the necessary practice time, one should also consider the likelihood of forgetting an authentication sequence and the time spent both by the device user and the security manager in assigning new sequences to users.

A significant question with any approach is whether participants are capable of remembering a set of sequences, not just one particular sequence. Users are often encouraged to select entirely different passwords for each system that requires one. An element of the *password problem* is not only that passwords should be easy to remember but hard to guess, but also that a user must be able to create many such passwords. As mobile devices and embedded touch screens become more prevalent, TAPI users would need to be able to remember many image sequences in order to authenticate. In order for TAPI to gain broad acceptance, it is likely that the image set would have to be standardized. A longer study involving multiple devices and image sequences could help to resolve this issue. Early research on this question has been mixed, with

some researchers finding that memorability of any particular image-based authentication sequence decreased when a group must be remembered [7] while others find that performance of images is still superior to that of text [2].

VII. Summary

As mobile devices become more commonplace for everyday computing tasks, user authentication and authorization to use a mobile device becomes more important. The prevailing PIN approach offers the user a simple numeric sequence that is easy to remember, fast to enter, but is prone to attack through guessing. We presented TAPI an image-based sequence for authentication technique for touch-screens as a possible alternative to the PIN. TAPI presents the user with 64 possible choices at each point in the sequence by partitioning 16 images into 4 sections, increasing the number of possible combinations by a factor of 100 (from 10^5 to over 10^7). In a user study of TAPI in which sequences were randomly assigned to participants, 90% of users were able to remember their authentication sequences after one week on non-use and on a very recent small touch-screen, demonstrated a median best entry time of 3.5s. A number of design alterations and future research directions exist to further examine the viability of TAPI.

Acknowledgment

We wish to thank Heather Richter Lipford for her suggestions and comments about an earlier draft of this work.

References

[1] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords? A field trial investigation," in *People and Computers XIV - Usability or Else - HCI 2000*, 2000, pp. 405–424.

[2] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in *Proc. ACM Conf. on Comp. and Comm. Security*, Chicago, Illinois, USA, 2009, pp. 500–511.

[3] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int'l J. Human-Computer Studies*, vol. 63, nos. 1-2, pp. 128–152, 2005.

[4] J. Deregowski and G. Jahoda, "Efficacy of objects, pictures and words in a simple learning task," *Int'l. J. Psychology*, vol. 10, no. 1, pp.19–25, 1975.

[5] R. Dhamija and A. Perrig, "Deja vu: a user study using images for authentication," in *Proc. USENIX Security Symposium*, Denver, Colorado, USA, 2000, pp. 45–48.

[6] A. Dirik, N. Memon, and J. Birget, "Modeling user choice in the PassPoints graphical password scheme," in *Proc. ACM SOUPS*, Pittsburgh, Pennsylvania, USA, 2007, pp. 20–28.

[7] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in *Proc. CHI - Int'l Conf. on Human Factors in Computing Systems*, Boston, Massachusetts, USA, 2009, pp. 889–898.

[8] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Tech. Rep. NISTIR 7030, July 2003.

[9] W. Jansen, S. Gavrila, V. Korolev, T. Heute, and C. Séveillac, "A Unified Framework for Mobile Device Security," in *Proc. SAM – Int'l. Conf. Security and Management*, Las Vegas, Nevada, USA, 2004.

[10] S. Komanduri and D. R. Hutchings, "Order and entropy in picture passwords," in *Proc. Graphics Interface*, Windsor, Ontario, Canada, 2008, pp. 115–122.

[11] J. B. Horrigan (2009, July 22). "Press Release: Mobile internet use increases sharply in 2009 as more than half of all Americans have gotten online by some wireless means," Pew Internet & American Life Project [Online]. Available: http://www.pewinternet.org/Press-Releases/2009/Mobile-internet-use.aspx

[12] J. Snodgrass and B. McCullough, "The role of visual similarity in picture categorization," *J. Experimental Psychology: Learning, Memory, and Cognition*, vol. 12, no. 1, pp. 147–154, 1986.

[13] T. Takada, T. Onuki, and H. Koike, "Awase-E: recognition-based image authentication scheme using users' personal photographs," in *Proc. Innovations in Info. Tech.*, Dubai, United Arab Emirates, 2006, pp. 1–5.

[14] J. Thorpe and P. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," *Proc. Usenix Security Symp.*, Boston, Massachusetts, USA, 2007, pp. 103–118.

[15] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: basic results," In *Human-Computer Interaction International*, Las Vegas, Nevada, USA, 2005.

[16] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: effects of tolerance and image choice," in *Proc. ACM SOUPS*, Pittsburgh, Pennsylvania, USA, 2005, pp. 1–12.

[17] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: design and longitudinal evaluation of a graphical password system," *Int'l. J. Human-Computer Studies*, vol. 63, no. 1-2, pp. 102–107, 2005.

[18] T-Mobile G1 Overview (2010 Feb. 13) [Online] Available: http://www.t-mobileg1.com/g1-learn-overview.aspx