Keeping Secrets from Friends: Design Guidelines for Multiplexed Graphical Passwords

Ian Oakley[1], Andrea Bianchi[2]

[1] Ulsan National Institute of Science and Technology, Department of Human and Systems Engineering, Ulsan, Korea.

[2] Sungkyunkwan Unversity, School of Information and Communication Engineering, Suwon, Korea.

Abstract

Background Entering passwords on mobile devices often takes place in public, situations in which input actions are exposed to the people around you and passwords can be compromised simply by sneaky glances over shoulders. However, the people who surround a user are typically not malicious attackers seeking to steal data, but rather friends and colleagues. This article characterizes such individuals as casual observers and describes the threats they pose to security and password integrity.

Methods Based on an analysis of the literature and design space, we introduce a systematic framework for multiplexed authentication, a term we introduce to describe a class of systems that maintain security against the threats posed by casual observers through obsfuscated input. Building on this knowledge, we present a set of design dimensions and guidelines for multiplexed graphical passwords. Finally, we present ShaPIN, a multiplexed input prototype designed in light of these guidelines and that aims to protect users against casual observation.

Results Evaluations of ShaPIN with a user study reveal it can be used rapidly, accurately and that it provides protection against in-person observation. ShaPIN also offers substantial performance imporvements over prior systems in its class, evidence that helps support and validate our design framework.

Conclusion We believe that the framework of multiplexed authentication can inform and shape future work to ensure that passwords stay safe and secret in front of friends. By presenting design guidelines for multiplexed graphical passwords we also hope to raise awareness of the important issue of password security in the design community and to show how design research can innovate in this area to create more usable and effective password systems.

Keywords Casual Observer, Password Design, Dsign Guidelines, Multiplexed Input.

*Corresponding author: Andrea Bianchi (andrea.whites@gmail.com)

This work was supported by the National Research Foundation of Korea (NRF) Basic Science Research Program grant funded by MOE (NRF-2010-0020210), the NRF grant program funded by MEST (NRF-2014-002223) and the year of 2013 Research Fund of the Ulsan National Institute of Science and Technology (UNIST).

Citation: Oakley, I., & Bianchi, A. (2014). Keeping Secrets from Friends: Design Guidelines for Multiplexed Graphical Passwords. *Archives of Design Research, 27*(3), 49-63.

http://dx.doi.org/10.15187/adr.2014.08.111.3.49

Received Jul. 15. 2014 **reviewed :** Jul. 25. 2014 **Accepted :** Jul. 25. 2014
pISSN 1226-8046 **eISSN** 2288-2987

1. Introduction

Look away! When your colleagues are logging in to their computers, that's how the US Department of Homeland Security recommends you behave.

After all, they continue, those passwords are protecting national secrets so its only "common courtesy" (Huth, 2013) to avert your eyes. Jacob Nielsen (2009), a prominent design usability guru, seems to agree. He argues password masking, the common practice of substituting entered password characters with unintelligible asterisks in web forms, violates usability principles and should be stopped. How many passwords, he asks, are really stolen via observation, via surreptitious glances that peak over shoulders? Bruce Schenier (2014), a leading figure and author in practical computer security, paints a more nuanced picture. The importance of observation attacks depends on the context of use - there is little risk when users are entering long, complex encryption keys in the privacy of their own homes.

But when out and about, accessing devices and services in public places or operating public terminals such as ATMs, it is a different story. Moreover, not only are users surrounded by strangers, but also potentially by peers, co-workers and friends - should the secrecy of our passwords be protected simply by the social convention that other users will avert their gaze or should we design technologies that protect passwords from these kinds of casual, and most likely benevolent, observers?

In fact, password observation is an important issue for pervasive mobile and wearable intearctive devices. These personal tools manage and access increasing quantities of important and potentially sensitive information - email accounts, banking applications and social networking services. They are also used in an incredibly wide range of public contexts and with almost unprecedented frequency - recent estimates suggest users open their mobiles phones up to 150 times per day (Meeker, 2013), or roughly once every five to ten waking minutes. Furthermore, many applications on a mobile are protected only by the system level password - after a device is unlocked the majority of its contents, features, data and services are freely and fully available. In reality, we argue that publicly exposing device passwords is far from a desirable situation.

Despite these concerns, and in stark contrast to the arcane password policies present in most desktop computing environments, many users intentionally opt for simplistic password schemes for their devices - or none at all. Possibly due to the frequency with which devices are accessed, or a perception of safety conferred via possession, security is typically seen as obstructing a user's activity and work (Sasse, 2011). Reflecting this trend towards simplicity, companies have introduced lightweight, rapid authentication systems for mobiles. A prominent example is the Android pattern lock (Figure 1, left), a graphical password scheme in which users make a single stroke to connect between two and nine dots arranged in a grid. Its quick, error tolerant and highly popular. It also offers negligible resistance to observation – a single glance can be enough to learn a password and even post-hoc observation, based on examining the smears left on the touch-screen, can be effectively used to extract the secret pattern (Aviv, 2010).

This weakness poses particular issues for what we term casual observers - the colleagues and peers who may accidentally learn passwords simply by failing to look away at the critical moment of entry. Given the growing and preferential use of tablets, mobiles and other pervasive devices in entertainment and collaborative work activities and indeed the physical sharing of such devices during these tasks (Rogers, 2009), we argue that is not always possible to maintain the Department of Homeland Security's recommended etiquette. Even without malicious motives, looking away is not as easy as it sounds and not knowing can become a chore. This is problematic as, beyond the fundamental security issues, conspicuously protecting passwords (such as cupping a hand around the input field, as in Figure 1, right) or inadvertently revealing or learning them can result in social discomfort, embarrassment or awkwardness (Sasse, 2011).

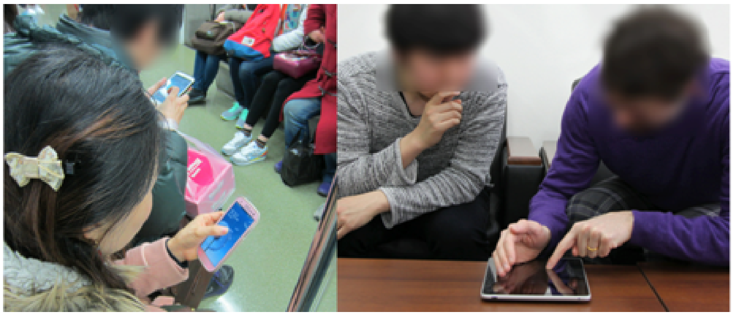

Figure 1 Two casual observation scenarios. On the left, a user authenticates with the Android Pattern Lock on a busy subway. On the right, a user conceals his password entry process from a colleague by cupping his hand over a tablet screen.

To address these issues, this article discusses interaction techniques that provide resistance to in-person observation. It focuses on protecting passwords from casual observers, benevolent peers who are near a user during authentication, by introducing multiplexed authentication, a novel framing for systems that feature visually obfuscated input. We then draw out key design dimensions of the space, highlight tradeoffs and make recommendations in the form of a defined set of design guidelines for future systems. We conclude by describing two recent multiplexed authentication schemes we have implemented and summarize the results of the studies we have conducted on them.

2. Casual Observers

In computer security, attackers are typically viewed as nefarious, dedicated and smart. Security schemes need consider the worst possible scenarios to be effective and, in the research community, there are kudos to be gained by coming up with novel ways to crack existing systems. Common standards have emerged for the threat models by which systems can be attacked. For basic techniques such as brute force guessing, the required security level varies with the use context - for systems on public terminals, schemes with 10,000 possible passwords (e.g. four digit ATM PINs) are common. In contrast, online systems, which can be subject to exhaustive, automated remote attacks, typically use much larger password spaces. Mobile devices, with their focus on the usability of authentication interfaces and the additional implicit security conferred by device possession tend to focus on the lower end of this scale.

There are fewer standards for observation resistance, but typical studies assume attackers with access to clear, high-resolution video of users making one or more successful authentications and ample time to review and extract password contents through careful analysis of this media. However, just like required resistance to brute-force attack varies from situation to situation, we argue that resistance to observation is best defined contextually. Other researchers agree. Hayashi et al. (2013) reveals that more than half of the logins on mobile devices happen at home or work, locations they characterize as low risk and suitable for relatively weak authentication schemes with a high level of usability. One component of this argument is simply that the people that surround a user in these environments are family members, friends and colleagues - individuals who, despite their proximity, are very unlikely to intentionally steal passwords. This article characterizes these individuals as casual observers and the threat they pose as one of inadvertently discovering passwords by failing to maintain privacy preserving behaviors such as averting their eyes when another users authenticates. In this framing, the goal of providing resistance to observation is not to lock down a system against a dedicated attacker, but to ensure that benevolent individuals who accidentally observe user authentications remain ignorant of password contents.

Distilling this discussion into concrete conclusions, we isolate four specific qualities of the casual observation threat model. Firstly, casual observers are non-malicious. Secondly, they observe password entry in person and close-up, often while sharing the same device. Thirdly, they take no notes nor record any video of entry processes. Fourthly, as long-term peers of a user, they are exposed to repeated observations of authentication sessions, both in a single sitting and over time. While this model differs considerably from traditional security threat models, we believe it has value in identifying, exposing and ultimately designing to tackle the predominantly social issues around unintentional password disclosure to peers.

3. Multiplexed passwords schemes

Guarding against casual observers involves making input that is undisclosed or ambiguous to a nearby person capable of seeing every part of the interaction: hands, screen and pointing device. One way to achieve this is to design interfaces that map a single input event to multiple on-screen password items. In this way, an individual who observes the authentication is unable to determine exactly what password item was selected by any given input. In this article, we introduce the term *multiplexed authentication* to refer to these systems. The name reflects the fact that a user's intended selection is mixed and combined with one or more alternatives in order to obfuscate their password.

Reflecting the importance of observation as a security threat, the literature provides a range of examples of multiplexed systems. In some of the earliest work on this idea, Tan and colleagues (2005) presented a spy-resistant keyboard based on a 14 by 3 grid of tiles each containing a set of three random characters. One character in each tile was always highlighted and users made selections by toggling through the highlighted items in conjunction with selecting a specific tile. In this way, neither the highlight nor the tile selection was sufficient for an observer to determine which character was selected - both had to be combined. Roth and colleagues (2004) proposed a conceptually related system for numeric PIN entry. It featured a standard numeric keypad, with a random set of half of the keys colored black and remainder colored white. Instead of tapping numbers, users repeatedly selected the colors of their PIN items. After three or four complete PIN entries (12 to 16 individual selections) the system could capture sufficient information to disambiguate the PIN, a feat the authors suggest that human observers would not be able to replicate. A more recent example is de Luca and colleagues' ColorPIN (de Luca, 2010). It is based on a novel type of PIN composed of four number-color pairs (e.g. three-red or seven-black).

It appears on screen as a large numeric keypad with three small alphabetic characters in three colors (black, white and red) underneath each digit. The characters repeat, so that each appears under three different keys, once in each different color. Users type the characters on a keyboard to select associated number-color pairs, a process that that confounds observation - each character input relates to three possible selections.

Similar concepts have been applied to graphical passwords. One example is the Convex Hull Click (CHC) scheme (Wiedenback, 2006). In this system, many small icons are randomly positioned on screen. Most are superfluous, but between three and five of these belong to a user's password. To enter a password item, users must locate at least three of their icons and click within the polygon they outline. As the click does not clearly relate to any of the icons shown, it is hard for an observer to deduce the password. Finally, PicassoPass (van Eekelen, 2013) is a recent and unevaluated example. It is based on a fixed grid of 12 compound icons each featuring a random color, shape, theme and character. A password is composed of individual elements, such as a shape or character, which users select by touching the compound item that contains them. Because all the content visually overlaps, an observer cannot distinguish which aspect of the compound icon a user actually selected and which aspects were present only incidentally.

In summary, as this persistent research interest suggests, multiplexed authentication is a promising technique for increasing resistance to observation. But many issues remain. Compared to standard authentication interfaces, multiplexed systems trade usability for security. This becomes painfully clear via a cursory examination of password entry times for typical systems. These are reported to be between 13.5 (de Luca, 2010) and 71 (Wiedenback, 2006) seconds, arguably too long for users in most tasks.

To try to understand why, and isolate avenues for improvement, we present and discuss six design dimensions of multiplexed authentication system, providing practical guideance and reccomendations for each. The goal is expose the common elements underlying such systems and shed light on how performance can be boosted without sacrificing security. We intend this discussion to frame future work on multiplexed authentication by making recommendations for increasing the efficiency and effectiveness of this class of system. The design dimensions and guidelines are presented in the next section.

4. Design guidelines for multiplexed input with graphical passwords

Randomization: A key element of multiplexed authentication is that interface components are randomly arranged on screen - buttons and icons are shuffled or colors and images are swapped. Without this randomization, an attacker would only have to note the physical movements a user performed in order to replicate the password - much like the status quo. However, because the elements are randomized users must process the displayed content to inform a decision about what to select. To maximize this behavior, in most current multiplexed systems, screen contents are randomized after every selection, multiple times during the course of entering a password (e.g. 10, 11, 12). While this is effective, it is also laborious and potentially cognitively taxing. We suggest that minimizing the use of randomization, ideally so that it occurs only once per full password entry (e.g., 13), is a desirable design goal that will improve the performance of multiplexed systems.

Indirectness of Input: To enable selection of multiple on-screen elements via a single input action most current multiplexed systems require user's make selections via a proxy - some distant interface element or tool. For example, in ColorPIN (de Luca, 2010) users don't select number-color pairs directly, but they type on a keyboard the characters that are associated with them; in CHC (Wiedenback, 2006) users don't select the icons in their password, but the space surrounding them. While this input indirection is the foundation of many multiplexed schemes, it also inherently presents users with a challenging task of mapping, processing or reconfiguring the displayed contents to determine what or where their actual input should be.

This contrasts strongly with the simplicity of traditional direct selection authentication schemes - at the ATM "1" clearly and effectively signifies "1". Accordingly, we argue that efforts to increase the directness of input mappings will increase the usability, and particularly the efficiency, of multiplexed schemes.

Cognitive challenge: Authors have posed users with a range of cognitive challenges (sometimes called trapdoor games (Roth, 2004)) in order to achieve input indirection. In the simplest, users must recognize some quality of their password item - its color or shape for example. In more sophisticated systems, users must process or integrate information, such as determining the next tab highlight in Tan's spy-resistant keyboard (2005).

Finally, systems such as CHC (Wiedenback, 2006) pose even more complex tasks involving spatial cognition to determine what points are enclosed by a polygon. The security literature, as well as general HCI guidelines, suggests that simpler cognitive tasks are more rapidly and reliably performed. Recognition tasks, in which users select their password items from a set of visually presented possibilities, are typically viewed as optimal choices. As such, we suggest that multiplexed authentication systems should be designed around recognition tasks in order to support optimal performance.

Category Count: Multiplexed schemes typically involve multiple orthogonal categories of password item - for example, the highlight and tiles of Tan's spy-resistant keyboard (2005) or the colors and numbers of de Luca's ColorPin (2010). The numbers of categories that appear vary considerably, ranging from the single black/white category of Roth's PIN entry system (2004), to the five distinct categories of PicassoPass (van Eekelen, 2013). In general, systems with a greater number of categories have more ambiguity in the interface and support a larger number of possible passwords. Consequently, it is harder for an observer to infer user password items from user input. However, as more categories are introduced, the complexity of the content increases. A likely consequence is that the conspicuity (Wertheim, 2010), or ease with which individual elements can be distinguished or recognized will drop, lowering system usability. In choosing a number of categories to use in a system, designers need strike a balance between simplicity and security.

Category Cardinality: The categories used in existing multiplexed systems feature very different cardinalities, or numbers of unique cues.

In the work reviewed in this paper, category cardinality ranges from a minimal three colors (de Luca, 2010) to an overwhelming 42 tiles (Tan, 2005). The implications of category cardinality are broad. For example, higher cardinalities increase the resistance of a password system to brute-force attacks that attempt to exhaustively enter passwords - there are simply more possibilities to consider. However, higher cardinalities require greater search, recognition and decision time. It is easy and quick to make the binary distinction between Roth's black and white keys. But in the case of the 12 colors used in PicassoPass, its likely that the human capacity for reliable absolute judgment is overloaded and, even if not, well established principles, such as the Hick-Hyman law (Cockburn, 2007), mathematically link greater numbers of options to lengthier decision times. Designers need balance the category cardinalities they select between the constraints of the password space they delimitate and the ease and speed with which users can make selections.

Repeated Observation: Casual observers, unlike traditional malicious attackers, have prolonged exposure to users, potentially seeing multiple password entries up close. But an inherent feature of multiplexed schemes is that repeat observations provide additional information that can be used to disambiguate a password. Ultimately, a user always enters the same password and, regardless of the nature of the input multiplexing, a series of observations will eventually provide sufficient information to determine that password contents. A typical stance to deal with this issue is to assume that the complexity of achieving this longitudinal intersection is beyond the means or desires of a simply casual observer (Roth, 2004). This is a fair point, but a closer analysis of the interrelationship between the number of categories in a system and their cardinalities gives more nuance to this issue. Basically, there is a tradeoff between these qualities. To illustrate this point, consider a system in which a user can choose a four-item password by selecting buttons, each mapped to two cue categories (e.g. numbers and colors) with cardinalities of ten. Although the theoretical password space of such a system is very large (e.g. (10*2)2), it is very weak against repeated observation. This is because between two authentication sessions there is very little chance that cues from the two categories will overlap in the same way. As such, an observer will likely be able to correctly determine the password by simply identifying the sub-set of selected cues that appear in both sessions - the intersection of the total cue set selected in each individual session. The precise probability that this intersection will fully reveal the password can be determined by calculating the probability of non-mutually exclusive events where the base probability of the same pair of cues reappearing together is directly derived from their cardinality - 10% in this example. As such, with two ten-cardinality categories, the chance that one of four password items will repeat is just 19%. This means that more than 80% of the time, two observations of the system will be enough to reveal the full password.

Table 1 Exploring the tradeoff between number of categories and category cardinality in multiplexed authentication. For a range of possible system configurations the table reports resistance against 1) brute force attacks based on guessing the password contents 2) key guessing attacks based on selecting input elements at random and 3) the probability of determining a password after watching a user perform a single entry. It also shows the probability that there will be an overlap between displayed password cues on repeated authentications in a multiplexed systems. This is a good guideline for gauging system resistance against casual observers who may see a user authenticate frequently.

Categories	Cues	Brute force (1 in ···)	Key guessing (1 in ···)	Probability to crack after 1 observation	Probability of intersection	Notes
1	10	10000	10000	100	0%	Standard PIN
2	4	4096	256	6.3%	43%	Security weak also for casual observer.
2	5	10000	625	6.3%	36%	
4	4	65536	256	0.4%	68%	Guessing VS Observation attack trade-off
4	5	160000	625	0.4%	59%	ShaPIN
5	4	331776	256	0.1%	82%	Strong security but compromised usability
6	5	810000	625	0.1%	73%	

In contrast, consider a system with four item categories (e.g., a number, a number-color, a letter and a letter-color) each with a cardinality of three. In this system, the password space is relatively small ((4*3)4) but the chance that cue items will overlap across multiple authentication sessions, calculated as a non-mutually exclusive probability, is relatively high (80%).

As such it offers improved resistance to repeat observation, and particularly to casual non-malicious observers who are exposed to multiple sessions but take no notes and make no persistent efforts. This tradeoff, basically a balancing of resilience against observation with resistance to brute force attack is a final important design consideration for multiplexed password systems. To more fully characterize this issue, Table 1 presents figures for the security of multiplexed systems with a range of different category count and cardinality configurations. It considers different types of attack including brute-force, key guessing (just selecting keys or icons, rather than actual possible password items, at random) and observation.

5. ShaPIN prototype

In order to instantiate and explore these recommendations, we designed and developed two variations of ShaPIN, a multiplexed authentication system based on compound icons and shown in Figure 2. Practically, ShaPIN is composed of a five by five grid of icons intended for use with a touchscreen so that users can directly tap the icons to make selections. It was implemented on the Samsung Galaxy II Smartphone. Navigating the tradeoff between susceptibility to brute force and observation attacks presented in Table 1, we created four categories of information associated with each icon, each with a cardinality of five. The categories are: numbers (1-5), letters (A-E), colors (red, green, blue, yellow, cyan) and shapes (circle, square, triangle, four-pointed star and five-pointed star).

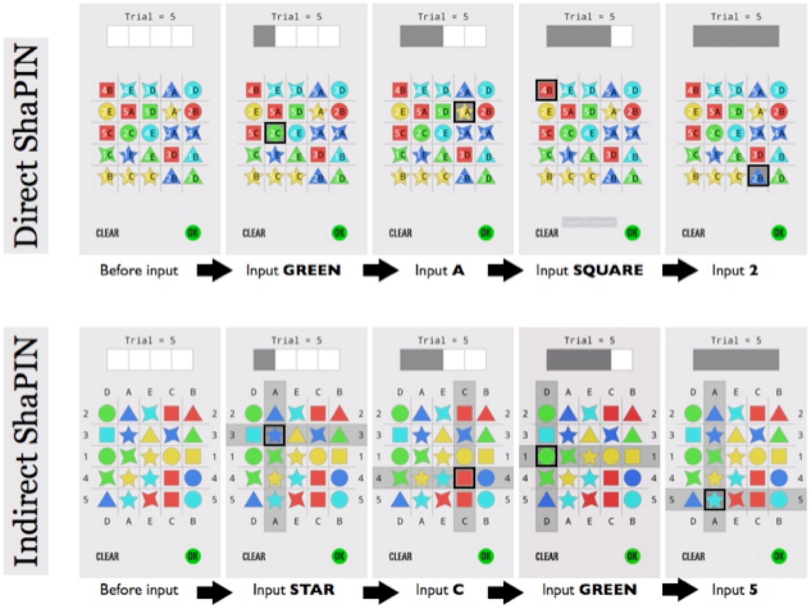

Figure 2 Screenshots of the direct ShaPIN (top) and partially indirect ShaPIN (bottom) interfaces. Both systems feature five cue categories (numbers, letters, shapes and colors) each with a cardinality of five items that are randomly but equally distributed over 25 selectable icons. In the direct interface all cues are shown within the icons, while in the indirect interface numbers and letters are associated with rows and columns to reduce visual clutter. The pictures above show how to insert a PIN composed of 4 items for each of the two password input systems.

Randomization is kept to a minimum and occurs only at the start of each authentication session. It involves each icon being assigned one value from each category with the constraint that every value from very category appears exactly five times over the entire grid. Finally, to explore the value of input directness in relation to the cost of increasing the density of visual information, we created a fully direct interface (Figure 2, left), in which cue assignments are fully random over the grid, and a partially indirect interface (Figure 2, right), in which numbers are shown at the top and bottom of the icon grid and letters to the left and right. Accordingly these cues are associated with their respective columns and rows of icons. In both versions of the system, password items are composed of four items from any of the categories. The interfaces also include a status bar to show progress as well as enter and cancel buttons.

6. Evaluation

We conducted two studies of the ShaPIN systems, assessing usability and security against observation. In the usability study, 12 student participants were compensated with approximately 5 USD to perform 20 authentications with each system in a fully balanced repeated measures design. The first five authentications were discarded as practice and we captured task times and error rates from the remaining 15 trials. If participants made an error, they were required to re-complete the trial. In total, the study involved entry of 360 correct passwords or 1440 correct password items. The results indicated the direct interface led to a mean task completion time of 5.81 seconds (SD: 1.24), while the partially indirect interface recorded 6.51 seconds (SD: 1.67), a difference that a paired t-test determined was significant (p=0.038).

Error rates for both systems were too low for formal analysis. A total of just four errors were recorded in the direct system (2.2%) and two errors in the indirect system (1.1%). Based on these data we concluded that the usability of the ShaPIN system is generally good. Compared to prior work on multiplexed authentication it is rapid and errors rates are extremely low for experimental settings. The direct interface shows modest, but significant improvements (12%) in completion time compared to the partially indirect system, suggesting that, in this case at least, a fully direct interface remains more readily intelligible than the less cluttered indirect version.

In the security study, two new participants completed five authentications with each system. During this process, one attacker was also present and free to visually observe the user's input in any way they choose. An experimenter also recorded unobstructed video of the device screen. To more closely resemble casual observers, attackers were selected to be students with no background in security and were furthermore prevented from taking notes of any form. After users completed five authentications, attackers were immediately given five attempts to enter the password. In the final stage of the study, the casual observer constraint was relaxed and attackers were presented with the video clips and asked to use any technique they wished to extract the passwords. There were allowed unlimited time and asked to provide a list of their top three guesses as to the password contents. In the shoulder-surfing portion of the study one attacker successfully entered the users password in the partially indirect ShaPIN interface three times (first, second and fourth attempts), suggesting she had partially cracked the password but remained uncertain regarding one or more of the items. Neither attacker cracked the direct interface. In the video portion of the study, one attacker cracked both passwords, while the other cracked one and correctly identified three PIN items in the second. They achieved this performance with their first guesses, clearly highlighting the weakness of the system against camera attack. In order to explain how the password was cracked in the partially indirect interface during shoulder surfing, we examined the password contents. It featured two numbers, one letter and one color. Examination of the video of this entry revealed that the user always selected each of the three alphanumeric cues by tapping on one of the appropriate edges of the grid - directly adjacent to the number or character in his password. We suggest that this additional cue was sufficient to readily reveal these three password items to the attacker. This finding highlights users' reliance on clear spatial mappings during interface use and reinforces the simplicity and benefits of direct mapping in multiplexed authentication systems.

In summary, these two studies validate the design guidelines presented in this article. By identifying the salient design issues in the space of multiplexed authentication we were able to create simple, effective systems that users could use rapidly and reliably. Compared to prior work on this topic, ShaPIN task times and error rates are laudably low. For example, some of the most rapid tasks times previously recorded for multiplexed schemes are from de Luca (2010) whose participants entered a password in a mean of 13.5 seconds, more than double the speed participants attained with ShaPIN.

Other schemes report longer entry times, from 23.3 seconds (Roth, 2004) through approximately 50 seconds (Tan, 2005) to 71 seconds (Wiedenback, 2006). While these schemes vary substantially in their design, making direct comparisons of experimental data of questionable validity, we argue that the rapid entry times achived in ShaPIN serves to validate the design framework and guideance presented in this paper – it enabled the creation of a relatively rapid, effective and potentially practical viable authentication system.

Furthermore, although the security study revealed weaknesses in one of the ShaPIN designs, it validated the core concept - multiplexed input makes it challenging for a casual observer to deduce a password, even after repeated viewings. However, as the video attack demonstrated, given ample time and access to recordings, cracking the passwords is inevitable - multiplexed input does not protect against dedicated and persistent attackers. It is valuable security technique only against single observation sessions or casual observers. If future designers, researchers and developers create multiplexed authenication schemes they need do so in light of a full and complete understanding of the limiations of the threat model outlined in this article. We argue that in other siutations multiplexed systems cannot effectively protect users and should not be deployed.

7. Conclusion

This article deals with authentication techniques suitable for pervasive computing scenarios - on mobiles or wearables and in everyday life. It argues that casual observers, a term it uses to refer to collocated but non-malicious peers, are a ubiquitous part of many common authentication contexts such as home and work environments. It isolates the qualities of these individuals, and discusses a framework and design guidelines for multiplexed authentication that offers a way of concealing passwords from them. By reviewing prior work on this topic, it draws out key aspects of the design space for these systems and uses this analysis to inform the development of ShaPIN, a novel multiplexed authentication system. Two studies characterize user performance and system security against observation, ultimately serving to validate and further refine the framework. Specifically, this work reinforces our suggestions that minimizing randomization and focusing on direct input mappings can optimize performance without impacting security. The high performance levels attained with ShaPIN also suggest that the number of categories and category cardinalities used are appropriate for multiplexed authentication systems. Basically, in order to strike a good balance between the size of the password space in a system and its resistance to observation, and the visual complexity of a system against the human capacity for absolute judgment, we recommend that future designers focus on multiplexed systems with approximately four to six categories, each with a cardinality of four to six items.

In conclusion, we believe that the work in this paper shows the promise of multiplexed authentication systems for securing against casual observers.

We hope that future developers and designers are able to build on the framework presented in this paper to create new authentication systems that allow users, as well as their colleagues, peers, family and friends, to freely enter their passwords, safe from embarrassment and able to look wherever they please.

Reference

1 Aviv, A., Gibson, K., Mossop, E., & Blaze, M. (2010). Smudge attacks on smartphone touch screens. *WOOT, 10, 1-7.*

2 Cockburn, A., Gutwin, C., & Greenberg, S. (2007, April). A predictive model of menu performance. In *Proceedings of the SIGCHI conference on Human factors in computing systems*(pp. 627-636).

3 De Luca, A., Hertzschuch, K., & Hussmann, H. (2010). ColorPIN: securing PIN entry through indirect input. In *Proceedings of CHI '10,* 1103-1106.

4 Hayashi, E., Das, S., Amini, S., Hong, J., & Oakley, I. (2013). Casa: context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 3).

5 Huth, A., Orlando, M., & Pesante, L. (2013). *Password Security, Protection, and Management. US-CERT United States Computer Emergency Readiness Team,* October 23, 2012 (revised: February 06, 2013).

6 Meeker, M., & Wu, L. (2013). *Internet Trends.* Retrieved Febraury, 2014, from https://www.kpcb.com/insights/2013-internet-trends.

7 Nielsen, J. (2009). *Stop Password Masking.* Retrieved Febraury, 2014, from http://www.nngroup.com/articles/stop-password-masking.

8 Rogers, Y, Lim, Y. K., Hazlewood, W. R., & Marshall, P. (2009). Equal opportunities: Do shareable interfaces promote more group participation than single users displays?. *Human-Computer Interaction, 24*(1-2), 79-116.

9 Roth, V., Richter, K., & Freidinger, R. (2004). A PIN-entry method resilient against shoulder surfing. *In Proceedings of the 11th ACM conference on Computer and communications security* (pp. 236-245).

10 Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' - a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19*(3), 122-131.

11 Schneier, B. (2009). The Pros and Cons of Password Masking. Retrieved Febraury, 2014, from https://www.schneier.com/blog/archives/2009/07/the_pros_and_co.html.

12 Tan, D. S., Keyani, P., & Czerwinski, M. (2005, November). Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future* (pp. 1-10). Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

13 van Eekelen, W. A., van den Elst, J., & Khan, V. J. (2013, April). Picassopass: a password scheme using a dynamically layered combination of graphical elements. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems* (pp. 1857-1862).

14 Wertheim, A. H. (2010). Visual conspicuity: a new simple standard, its reliability, validity and applicability. *Ergonomics, 53*(3), 421-442.

15 Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184).