Multi-Touch Authentication on Tabletops

David Kim, Paul Dunphy, Pam Briggs*, Jonathan Hook,

John Nicholson, James Nicholson*, Patrick Olivier

School of Computing Science
Culture Lab, Newcastle University, UK
{david.kim, p.m.dunphy, j.d.hook,
john.nicholson, p.l.olivier}@ncl.ac.uk

*School of Psychology and Sports Science
PACT Lab
Northumbria University, UK
{p.briggs, james.nicholson}@unn.ac.uk

ABSTRACT

The introduction of tabletop interfaces has given rise to the need for the development of secure and usable authentication techniques that are appropriate for the co-located collaborative settings for which they have been designed. Most commonly, user authentication is based on *something you know*, but this is a particular problem for tabletop interfaces, as they are particularly vulnerable to *shoulder surfing* given their remit to foster co-located collaboration. In other words, tabletop users would typically authenticate in full view of a number of observers. In this paper, we introduce and evaluate a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing. In our pilot work with users, and in our formal user-evaluation, one authentication scheme - Pressure-Grid - stood out, significantly enhancing shoulder surfing resistance when participants used it to enter both PINs and graphical passwords.

Author Keywords

User authentication, graphical passwords, shoulder surfing, multi-touch interaction

ACM Classification Keywords

D.4.6 Operating Systems: Security and Protection – Access controls, authentication; H.5.3 Information Interfaces an Presentation (e.g., HCI): Group and Organization Interfaces - Computer-supported cooperative work.

General Terms

Security, Human Factors, Design.

INTRODUCTION

Protracted interactions with computer-based technologies often begin with a process of user authentication. This process typically involves a knowledge-based exchange in which a user inputs some credentials known only to themselves (such as a Personal Identification Number (PIN), or an alphanumeric or graphical passwords). In public settings, the user is encouraged to shield this secret information from possible onlookers, and typically does so through body orientation, as this type of authentication is innately vulnerable to shoulder surfing. While such simple precautions can prove effective for an intimate single user, personal interface exchange, they are likely to prove problematic for shared interfaces such as digital tabletops that encourage simultaneous, co-present, multi-user authentication and engagement.

Tabletop interfaces are set to become commonplace as commercial products such as Microsoft Surface [12] start to appear. Such interactive tabletop systems are usually designed to afford co-located collaboration between groups of users, i.e. the tabletop becomes a communal work-space shared by a small group of friends or colleagues. The very motivation of such systems is to allow the entire collection of users good visual access to the whole tabletop display. Consequently, intrinsically private processes, such as authentication, present a significant design challenge. The challenge is made still more pressing by the social context of tabletop use - close colleagues will not wish to signal mistrust in their fellow users and are therefore less likely to adhere to proper security compliant behaviors (such as shielding PINs).

This design challenge assumes that tabletop applications will *require* authentication, and we are surely justified in making this assumption: there is an increasingly large research community addressing information privacy (e.g. [4] [23] [29]) and security (e.g. [5] [27] [20]) on interactive surfaces and public displays. Indeed, in developing the Surface, Microsoft anticipate applications that include financial transactions and other security sensitive interactions that most likely require differentiation between collaborators with different levels of security clearance [20]. A final point is that current and future surfaces feature a software development kit (SDK) that enables third party developers to create bespoke applications. If these new applications require user authentication, it is likely to involve *something you know* to some extent, even if only as a mechanism of *last resort*. Despite the potential of more elaborate hardware-based, or biometric protocols, knowledge-based authentication is already pervasive, low-cost and does not require additional hardware.

Motivated by this, we explore the properties of multi-touch authentication protocols that are resistant to observation at-

CHI 2010, April 10 – 15, 2010, Atlanta, Georgia, USA
Copyright 2010 ACM 978-1-60558-929-9/10/04...$10.00.

tacks (or *shoulder surfing*). Our contributions are: (i) to provide an evaluation of the vulnerability of conventional authentication methods to shoulder surfing attacks; and (ii) to consider both the key principles involved in the design of knowledge-based authentication schemes, particularly those suitable for multi-touch interaction, and to apply an understanding of user behavior in collaborative settings. A consideration of both sets of factors culminates in (iii) the design and evaluation of a set of authentication schemes that are the result of an initial exploration of the design space. These schemes range from simple manipulations designed to shield PIN entry, to more elaborate visual PINs and pressure-based systems that do not require accompanying shielding actions. The result of this design process is (iv) the formal analysis of one particularly promising mechanism – the *Pressure-Grid* – that in our evaluation effectively improved the observation resistance of existing mechanisms such as PIN and recognition-based graphical passwords.

RELATED WORK

As we've argued, tabletop interfaces and public displays potentially pose new challenges for knowledge-based authentication processes and recent research has begun to explore design solutions. One set of solutions demands the separation of private and public information across private (e.g. mobile device) and public displays respectively [5]. While such solutions are conceptually elegant, they do require the inclusion of additional devices. Other solutions involve the use of angle-dependent views on tabletops, using display masks, lenses or polarizing filters (e.g. [21] [17]) but significant disadvantages include the fact that either only few fixed angles are supported or special glasses must be worn by the users. Other solutions requiring special hardware have also been considered [6] [9] [18]. These solutions are likely to be more costly due to the additional hardware required.

In this paper we explore software-based solutions that do not rely on additional hardware and that can therefore be deemed suitable for the mass-market. Such solutions rely on the design of protocols that physically or conceptually obfuscate user input. Unfortunately, such obfuscations often sacrifice elements of usability as either comprehensibility or usage times are adversely affected. Baker [1] describes an entry mechanism where the user identifies a row or column in which each particular character of a memorized password resides (using a 6 × 6 matrix of randomly positioned characters). A drawback of this method is that while the user does not explicitly reveal their credentials, the interaction still leaks useful information over time. For example, by recording the grid state and action made by the user for each password character across multiple logins, an *intersection attack* (set intersection of all selected rows and columns for each character) could be performed to decipher each password character.

Roth et al. [16] describe a protocol to permit observation resistant entry of PINs in a *cognitive trapdoor game*. This involves the user performing rounds of a protocol where the PIN is not explicitly selected, but knowledge of the PIN is crucial to completion. However, a user study found that this increased login durations by a factor of ten over standard PIN entry. Tan et al. [27] developed an on-screen keyboard for public displays to protect against observation of alphanumeric passwords. Once again, this method incurred a heavy time penalty for legitimate users, with average login times (when using the enhancement) increasing by 50 seconds over those recorded by a control group.

Graphical passwords [25] are increasingly proposed as a usable knowledge-based authentication mechanism. Recognition based systems [15] [26] are highly intuitive and their designs are becoming increasingly standardized and understood. General schemes of this genre assign users a sequence of secret *key images* which comprise the authentication credentials of the user. At login, the user must recognize and select these amongst a number of *decoy images* or *foils*. Usability benefits center around the capacity of humans to reliably recognize (as opposed to recall) large numbers of images following relatively brief presentations of key images in a learning phase (e.g. [24]). *Passfaces* [14] is a commercial system based on this concept that also exploits innate human ability to recognize faces. The images presented in the login challenges are taken from a proprietary database of faces, and one user study reports impressive recognition rates over long periods of time [3]. A typical login challenge uses a 3×3 array of faces, of which one is a key image, and the rest decoys. The challenge is repeated until the user has demonstrated knowledge of all key images (typically four). Despite (and perhaps because of) the demonstrable usability benefits of graphical passwords, such recognition-based schemes are perceived to be vulnerable to shoulder surfing. Tari et. al. [28] compared the ability of an observer to carry out a shoulder surfing attack on Passfaces and alphanumeric passwords in a variety of configurations. Participants showed themselves to be capable of observing and remembering the Passfaces logins of others, especially when logins were performed with a mouse.

One graphical password scheme specifically designed to resist the shoulder surfing threat is the *Convex Hull Click* scheme [30]. Here the user is assigned a number of icons that they must locate among hundreds of decoy icons in a series of challenges. At each challenge the user must locate three icons and click within the convex hull formed by their on-screen positions. Following the recurring theme in this field of observation resistance incurring time penalties to the user, the average successful login duration was 72 seconds although users were accurate in recalling their graphical password.

DESIGN CONSIDERATIONS

A number of researchers have provided us with use-cases that establish the need for improved authentication in tabletop environments. For example, Smith and Piekarski [23] envision the use of multi-view displays in an employer-employee meeting at a digital tabletop where the employer has access to the employee's history file. In such examples, we can identify a number of key themes: firstly, people have different access rights because they exist in different levels of a hierarchy and fear the disclosure of information that should

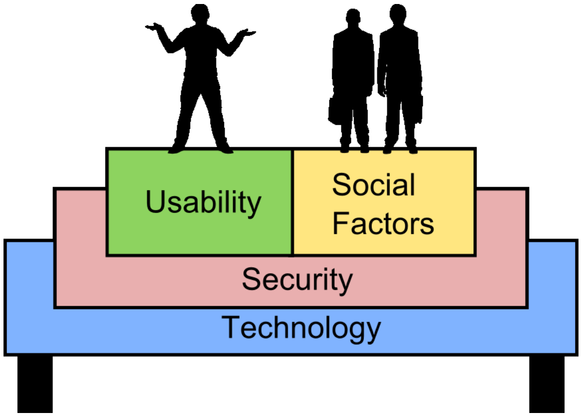


Figure 1. Important considerations for security mechanisms in co-located collaborative contexts.

be treated as confidential. Secondly, people may need to give others access to objects that can only be accessed via a personal gateway, where the login to that gateway should be kept confidential. In all cases, however, people respond to a social imperative that makes it difficult for them to signal an explicit mistrust of colleagues.

Within the public display or tabletop context, successful authentication rests, not only upon reliable system technology and effective security protocols, but also upon full system acceptability within a *social context* (Figure 1). Poor usability within this context can lead to either: (i) sloppy adherence to secure protocols on the part of the user (e.g. choosing easy passwords, taking notes); or (ii) users not using such protocols at all (e.g. not using access control). Similarly, poor understanding of the social and collaborative context in which authentication takes place can lead to assumptions about individual user behavior that are not born out in collaborative contexts. An accepted tenet in security research is the ease with which people can be persuaded into insecure behaviors simply because of normative social protocols [13].

Shoulder Surfing Resistance

Our goal is to design socially acceptable, but attack-resistant means of authentication for communal spaces. This raises the question of how we can make authentication comfortable for the user, but impenetrable for the observer? In practice, shoulder surfing can be hampered by interfering with one or more steps in the observer's processes of sense making and knowledge acquisition.

These can be summarized as follows:

1. **Reduce visibility:** reduce the saliency of areas on a display where sensitive actions are taking place. This can be achieved through additional hardware (e.g optical filters), forcing the user to cover input, computer graphics techniques (e.g. reduced visual quality, exploitation of orientation). Such approaches lead to minimal additions to the cognitive load on the user.
2. **Subdivide action:** subdivide the input action temporally or spatially and perform sub-actions sequentially (or concurrently when the action is divided spatially). In this way, the one-to-one mapping between one action and one part of the authentication key is removed, making actions harder to decipher for an observer lacking knowledge of user intentions. The disadvantage of this approach is that comprehensibility of the system is reduced for the legitimate user.
3. **Dissipate attention:** display redundant information to hinder the observer identifying information on the interface that is useful to memorize. However, the use of redundant information can negatively impact usability as the user must also navigate this information. Such systems are vulnerable to *intersection attacks* where an attacker records multiple logins and collates them in search of recurring patterns that can be used to uncover the credentials.
4. **Knowledge transformation:** enter the credentials in a form that is difficult, in isolation, to be used to reconstruct the correct credentials after observing a successful login. A key concern is that the transformation must be usable without excessive calculation from the user.

These approaches can be used to characterize the design space of existing and prospective authentication methods. Table 1 below, provides a comparison of a selection of proposed systems.

	Reduce visibility	Subdivide actions	Dissipate Attention	Transform knowledge
Non-disclosing authent. [1]			+	*
Cognitive Trapdoor Game [16]		*	+	
Spy-Resistant Keyboard [27]		+	*	
Convex Hull Click [30]			+	*
VibraPass [6]	+		*	

Table 1. Shoulder surfing resistance techniques used in other authentication methods (* = primary; + = supporting).

DESIGNS FOR MULTI-TOUCH AUTHENTICATION

Based on our set of approaches to reduce the likelihood of successful shoulder surfing attacks, we designed and implemented a number of multi-touch tabletop authentication schemes. Initially we sought secure numeric PINs, due to the fact they are already widely deployed and understood by users. We then proceeded to consider designs that were not constrained by text or number entry that permitted greater exploration of our suggested approaches.

The use of multi-touch interaction affords the possibility to exploit a number of qualities not available in traditional mobile and desktop settings. Firstly, visually complex bi-manual manipulations are relatively easy to perform but difficult to reproduce based on observation alone. Secondly, the physicality and directness of tabletop interaction means that interface elements can be directly touched and direct physical metaphors can be exploited – this could improve usability and comprehension of underlying security mechanisms. For example, one capability of many vision based multi-touch technologies is to track not only touch points but the contact area of hands on the surface. This enables systems to exploit meaningful gestures such as input shielding that clearly communicate their purpose. Thirdly, co-located users are likely to view content from very different angles. Finally, vision based multi-touch tabletop systems (e.g. FTIR [19]) can detect different levels of pressure applied.

Our threat model consists of resisting at least one shoulder surfing attack from an observer co-located at any position around the tabletop. Camera-based attacks are feasible with most knowledge-based authentication systems; but to defeat camera attacks was not our design goal. The pervasive nature of mobile devices instrumented with cameras is of particular concern, but as with other manifestations of this same problem (e.g. at the ATM) we rely upon social conventions to deter active attempts to video record logins.

Enhanced PIN Input

ShieldPIN

ShieldPIN incorporates a compulsory hand shielding gesture that provides a physical barrier to visibility. This is derived from a widely understood gesture associated with restricting the visibility of an item. This gesture forms part of an *interlock* mechanism that prevents the appearance of the PIN keypad until the gesture is detected in a hand-shaped zone on the interface. Upon detection, the keypad is displayed behind the shield (see Figure 2). This enables PIN entry with the remaining hand where shielding is designed into the interaction and is no longer a voluntary action that could be interpreted as an indicator of mistrust. The PIN keypad can appear and disappear in response to the detection of the shielding gesture. In practice the coverage provided by the gesture can be optimized, and it is likely that with some fine-tuning of the shape, orientation of the gesture, and size of the keypad, more coverage can be achieved.

The PIN entry process itself is unchanged which has significant usability and comprehensibility benefits. An observation attack on this method is likely to be difficult due to the small screen real estate used by the mechanism and the comparative size of shielding gesture. In the illustrated configuration (Figure 2) the assumption is that keypad visibility from the side uncovered by the shielding gesture is blocked by the hand entering the PIN. However, an attacker is most likely to be successful from a vantage point behind the shield. Wu and Balakrishnan use a similar mechanism in their room furniture layout application [31] to both invoke a special function and to provide privacy.

SlotPIN

The *SlotPIN* system is based on the principles of providing redundant information and encouraging concurrent actions (Figure 3). The user enters a PIN by aligning reels on the interface so that one row contains the correct PIN. The particular row is determined by the first (static) wheel. The task of the attacker is complicated by the order of numbers on all reels being randomized at each login. The user must manipulate the three remaining wheels to complete the alignment of the remaining PIN digits. The interface consists of four vertical reels of randomly ordered digits (0-9). This is similar in appearance to the historic *Jefferson Wheel Cipher*, and their behavior mirrors those in a *slot machine*. The wheels cannot be turned by direct interaction to reduce the likelihood that users directly touch – and reveal – each correct PIN digit. Instead a scroll wheel is provided below each of the three movable reels.

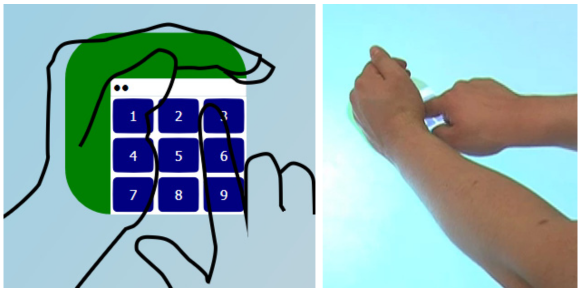
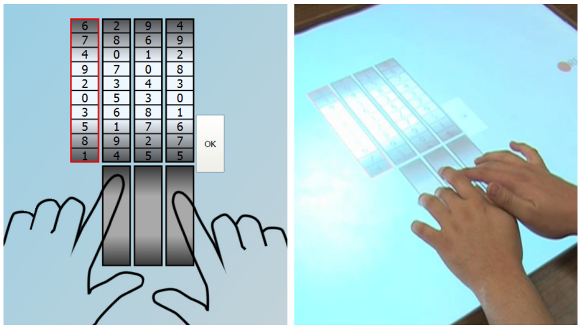


Figure 2. ShieldPIN screenshot with added example interaction (left), in situ (right): the PIN keypad only appears once the shielding gesture is detected in the green zone.



6	2	9	4
7	8	6	9
4	0	1	2
9	7	0	8
2	3	4	3
0	5	3	0
3	6	8	1
5	1	7	6
8	9	2	7
1	4	5	5

Figure 3. SlotPIN screenshot with added example interaction (left), in situ (right): attackers are confronted with decoy PINs.

In its current form SlotPIN is immune to one shoulder surfing attack, but has a vulnerability to multiple attacks. The best-case scenario for an attacker is that only 2 observed logins are required for success. After recording the end-state of one login, the attacker has 10 candidate PINs. Observing one further successful login in the best case will enable the attacker to find the PIN that the two logins have in common, this is an *intersection attack*. However, the randomized order of numbers on every reel at every login means there is a small possibility a decoy PIN will also re-appear. After one observation there is an approximately 1 in 1111 chance a decoy PIN will reappear and force the attacker to make another observation. Each observed successful login significantly shortens the list of candidate PINs gathered initially as each PIN that does not reappear can be eliminated. For this reason it is not a suitable deployment where camera-based attacks are a concern, but is an illustration of a number of the principles outlined previously.

CuePIN

CuePIN addresses the vulnerability of SlotPIN to intersection attack by combining features of both SlotPIN and ShieldPIN to add entropy to the final reel states. The shield gesture is used to create a covert channel between the system and the user so that each PIN digit can be aligned to a random row. The interface (see Figure 4) is visually similar to that of SlotPIN with the addition of an area to receive a shield gesture, and that *every* reel can now be manipulated by the user. Each row is also supplemented with an identifier character in the range A-J.

PIN entry proceeds as follows:

1. The user performs the shield gesture in a defined area to reveal a random character in the range A-J. The user removes their hand and the character disappears.
2. The user manipulates reel n to align PIN digit n to the row revealed by the shielding gesture.
3. Repeat 1 and 2 for each remaining reel until all PIN digits have been entered.

There are two elements that underpin the efficacy of this design: firstly, users are required to shield a much smaller area than in ShieldPIN (since only a single character is revealed) and this improves the secrecy of the shielding gesture. Secondly, the addition of the alphabetic characters at each position of the reel enables a random on-screen representation of the user's PIN. This method is resistant to multiple shoulder surfing attacks with or without a camera where an attacker fails to record both the shielded cue area and the final reel states. Without the sequence of shielded cues, knowledge of the end-state cannot be usefully applied in a replay attack.

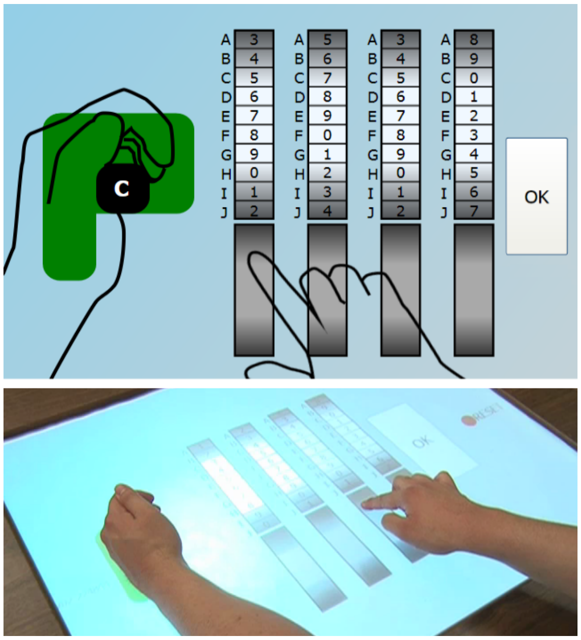
Multi-touch Graphical Passwords

The design space of graphical password systems has been extensively explored for mobile and single touch interaction. However, multi-touch interaction allows us to explore both parallel and sequential actions, thereby allowing us to design schemes that both obfuscate and explicitly hide PIN entry.

Color-Rings

Color-Rings is a visual authentication scheme that exploits both concurrent and redundant actions, presents redundant information and aims to restrict visibility through the size of objects on the interface. Unlike SlotPIN, that also employs concurrent and redundant actions, Color-Rings has this designed into the interaction. The interface is similar in appearance to the *Convex Hull Click* scheme [30]. The user is assigned i authentication icons called *key icons* that are collectively assigned one single color-ring: red, green, blue, or pink. At login the user is presented with i grids of icons where 72 icons are displayed per grid and one key icon is presented in each. Also at each login the position of the icons is randomized and distinct icons are displayed in each grid.

For each grid the user must *lasso* the key icon with the correctly colored ring, which is large enough to capture more than one icon. To begin the interaction the user is asked to place 4 fingers down on the display (ideally index finger and thumb from each hand) around which four rings of different colors are then drawn (see Figure 5). The user must drag all 4 rings concurrently and place them in the grid, three of the rings make decoy selections. Users confirm a selection by dropping the rings in position.



A	3	A	5	A	3	A	8
B	4	B	6	B	4	B	9
C	5	C	7	C	5	C	0
D	6	D	8	D	6	D	1
E	7	E	9	E	7	E	2
F	8	F	0	F	8	F	3
G	9	G	1	G	9	G	4
H	0	H	2	H	0	H	5
I	1	I	3	I	1	I	6
J	2	J	4	J	2	J	7

Figure 4. CuePIN screenshot with added example interaction (top), in situ (bottom): combines aspects of ShieldPIN and SlotPIN. Users are presented with a secret cue via the shield gesture to enable random alignment of each PIN digit.

To perform a random guess attack the password space is significantly larger than PIN due to the two tasks of discovering the correct ring, and the correct icons in each grid. The task of deciphering the information on-screen we believe to be too difficult based on short-term memory. Key determinants of security are the number of rings n, number of grids g, number of distinct icons in a grid i and capacity of the rings c. A random guess has a probability of $(\frac{1}{n} \times \frac{c}{i})^g$ of success which is significantly less than PIN where $n = 4$, $c = 5$, $i = 72$, $g = 4$. Clearly, knowing the correct ring increases this probability. A camera-based attack is potentially feasible over multiple logins. This is complicated due to the small size of the icons, and we suspect a high-resolution tabletop display and a good camera are prerequisites. After recording a single successful login the attacker has narrowed down the password space to $(n \times c)^g$ possibilities, which is still greater than that of a random PIN where $c = 5$, $n = 4$, $g = 4$, $i = 72$.

In practice, Color-Rings introduces additional cognitive load to the user as a result of the need to make the association between the color and key icons. In terms of both usability and accessibility the scheme requires hand dexterity, and shares issues with the *Convex Hull Click* scheme as it requires a potentially tiresome visual search to find the correct icon.

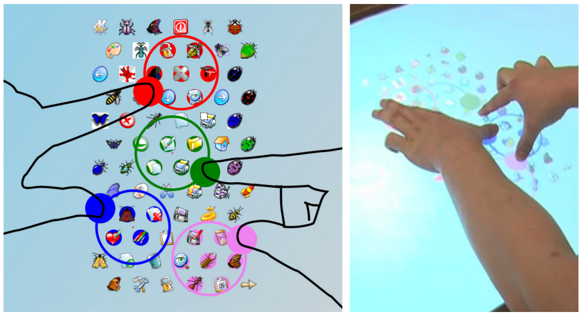


Figure 5. Color-Rings screenshot with added example interaction (left), in situ (right): The user drags colored rings to select key icons amongst decoys. Exploits concurrent & redundant actions.

Pressure Passwords

Vision-based multi-touch systems can obtain the size of the finger contact (or *blob*) detected by the camera. This means that changes in finger pressure can be harnessed. Such pressure differences are readily apparent to the tracking systems but are very difficult for observers to discern. This is improved by the fact that increasing pressure on some fingers (particularly the less dexterous fingers), causes involuntary movement on other fingers that is likely to further confuse an observer. This principle can form the basis of low-visibility interactions with a system.

Pressure-Grid

Pressure-Grid (see Figure 6) is a novel multi-purpose input mechanism that exploits this low visibility of changes in finger pressure for purposes of inputting PINs, recognition-based graphical passwords, or any other objects that can be displayed in a grid.

The user begins by placing three fingers of each hand in calibration areas on the interface. The system uses the locations of these touch points to dynamically draw the grid of objects, and pressure zones that are assigned to each finger – the dimensions of which are dynamically customized by the size of the hands and the spacing between fingers. This can sometimes result in pressure zones with slightly irregular shapes. In the implementation we chose a static pressure threshold to distinguish resting fingers and those exerting additional pressure. However, in future the pressure values recorded in the calibration step should be used to assign each finger an individual threshold as the strength and size of a finger impacts the pressure that can be applied. We chose to design for three fingers per hand due to informal observations that the muscles of the 4th and 3rd fingers lack independent dexterity, and that no masking movement results from pressure applied by the thumb. For these reasons, in our prototype, the interaction involves only the 1st, 2nd, and 3rd fingers of each hand. Once the grid is drawn, the user is presented with an $N \times N$ grid of objects where N corresponds to the number of fingers per hand used in the interaction.

Each cell is referenced by a (x, y) coordinate where x increases from left-to-right and y from bottom-to-top. Each finger on the left hand is assigned the corresponding value of y and those on the right hand values of x. For example on the right hand the 3rd finger is assigned $x = 3$, the 2nd $x = 2$ and the 1st $x = 1$. To select a particular cell, the user must apply additional pressure on one finger per hand. The system can attribute this additional pressure to particular pressure zones, and thus derive an (x, y) coordinate, which can be interpreted as selection of object (x, y). This can be repeated until an entire sequence of objects is selected. If fingers are completely removed from the table during the input, the login is canceled as the user may be at risk of exposing selections. One additional method used to increase the difficulty of observing finger pressure, is that the pressure zones constantly and randomly change color. The key element that underpins the security of this technique is that attackers will have difficulty attending simultaneously to sources of pressure from both hands and the object to which the pressure maps.

Malek et al. [9] present a *Draw a Secret* [8] style system that incorporates pressure sensitivity into the password encoding. Pressure-Grid differs from this scheme as it exploits multi-touch interaction, and does not require pen input. Also, different from Baker [1] the user is able to select a row and column simultaneously. Martino et al. [11] impose added cognitive load on the user as they are required to remember a combination of symbols, and a particular pattern with which to align them in a grid. The Pressure Grid is intended to support discreet selection of a multitude of object types and imposes no added cognitive load.

One possible limitation of this approach is in terms of accessibility as it requires good dexterity of the hands. Despite this, we believe it to be a promising solution to co-located observation attacks. A camera attack also seems difficult, although one useful approach could exploit technology described by Marshall et. al. [10]. This is where cameras are used to detect the change in color of flesh beneath the fingernail, caused by pressure of the finger upon a surface.

EVALUATION

We can conceptually evaluate the schemes we proposed by assessing them in terms of the four approaches to limiting shoulder surfing that we suggested earlier (see Table 2). A preliminary analysis indicates that Pressure-Grid potentially offers an all-round solution.

In early user-based pilot work, the Pressure-Grid was well-regarded, as it offered intuitive input and seemed to offer consistent resistance to shoulder surfing. We believed that the most likely real-world manifestations of the Pressure-Grid based on current research trends included the PIN, and recognition-based graphical passwords due to the similar interactions involved. This motivated our decision to evaluate the Pressure Grid in both contexts. We created a *Faces* graphical password system to mimic the Passfaces system which is a prominent exemplar of this genre of graphical password. In addition for the reason that human face recognition has the interesting property that it is heavily orientation-dependent [22]. We compared four configurations in a user

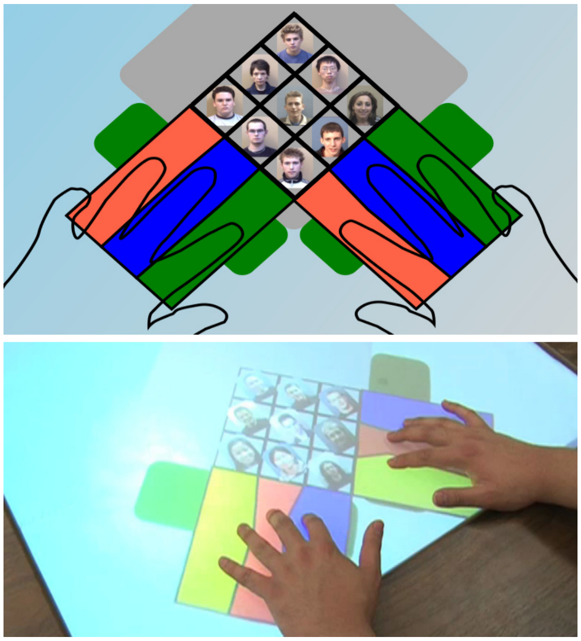


Figure 6. PressureFaces screenshot with added example interaction (top), photo (bottom). The user increases pressure on one finger per hand in the colored pressure zones to communicate an (x, y) coordinate and select an object.

study, using a novel design that simulated a shoulder surfing attack: basic (unshielded) PIN, basic (unshielded) Faces, PressurePIN and PressureFaces. Only a small number of user studies have attempted to model a shoulder surfing scenario, as such we chose a set-up similar to that described by Tari et al. [28], where participants perform a shoulder surfing attack on *live* input.

	Restrict visibility	Subdivide actions	Dissipate Attention	Transform knowledge
ShieldPIN	*			
CuePIN	*	+	+	+
SlotPIN		+	*	
Color-Rings	+		*	+
Pressure-Grid	*	+	+	

Table 2. Shoulder surfing resistance methods of established authentication methods (* = primary; + = supporting).

One key operational difference between PINs and Passfaces is that traditional PINs are entered on keypads with fixed digit positions, whereas Passfaces randomizes locations of faces at each login. This difference was included when implementing both Faces and PressureFaces. This means that using either of these systems, a shoulder surfer cannot rely solely on observing the hand positions of the user.

Procedure

21 participants (undergraduate and graduate students) were recruited to take part in the study. Each participant was exposed to each of the four systems in a within-subjects design. Each mechanism was randomly assigned a correct authentication sequence in advance, and instrumented to record timings of each login (from the first touch to the last touch), and the accuracy of the input. The study was filmed, but purely to record interesting participant behavior, as we worked with the assumption that camera attacks were feasible.

The procedure was as follows:

1. Groups of 3 participants were invited to each one hour session, the protocol of the experiment was explained, and participants were given time to familiarize themselves with each of the 4 systems.
2. One participant was randomly given the role of inputter for the entire session, while the remaining two were assigned as observers (attackers).
3. An authentication method was chosen at random, and the inputter given time to master the entry of the correct credentials for the chosen system. This was judged by successful input three times consecutively.
4. The observers then returned to the interface, and the inputter was asked to achieve 3 consecutive successful logins in the presence of the two observers. Mistakes by the inputter were ignored and the observers were able to take up any position around the table.
5. The observers then performed a 30 second distractor task (reading a short text) before being invited back individually (again in random order) to attempt to re-create what they had seen. The use of a distractor task is common in memory studies, often in lieu of a lengthy delay between observation and recall. Its use here was motivated by our assumption that an attacker cannot immediately make use of observed information, and may be required to retain the information over an extended time period or perform other tasks before they can commence an attack.
6. Each observer had three attempts to input the credentials observed. If successful in less than three attempts they were not required to login again using that system.
7. Steps 3-5 were repeated for each of the four systems.

The custom FTIR tabletop system [19] used, and a typical positioning of the *inputter* and *observers* are displayed in Figure 7.

RESULTS

The key results are summarized in Figure 8. Surprisingly only 10 of the 14 observers (71%) were able to login using an observed PIN. Those that failed commented that they either forgot the PIN between their observation and the opportunity for input, or that they simply made a mistake during the observation phase. Despite this, the PIN was still considerably more vulnerable to observation than the remaining three systems, confirming our earlier assumption that this mechanism in its traditional form is not appropriate for authentication in such public contexts. Faces was considerably more resistant to shoulder surfing with only 3 observers

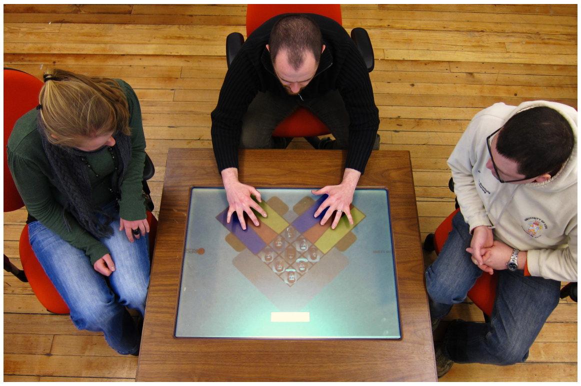


Figure 7. The FTIR table used for the evaluation $49 \times 95 \times 105cm$, and the user study context.

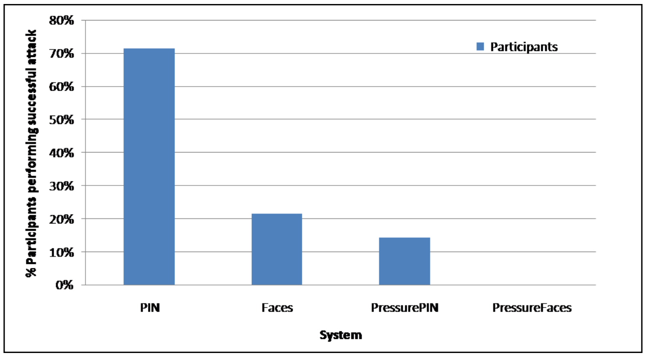


Figure 8. Percentages of observers able to replicate the inputter's credentials (by authentication method).

		Components Guessed				
System	**Logins**	**0**	**1**	**2**	**3**	**All**
PIN	22	14%	18%	14%	9%	45%
Faces	36	25%	19%	36%	11%	8%
Press.PIN	38	42%	32%	18%	3%	5%
Press.Fa.	42	57%	40%	2%	0%	0%

Table 3. Rounded percentage of logins where participants guessed a particular number of authentication components (138 attempts collected across all systems).

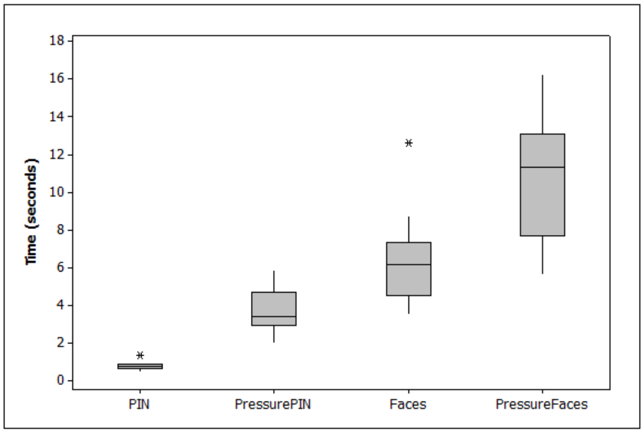


Figure 9. The distribution of successful login durations recorded for inputters per system.

(21%) able to login successfully. This could be due to the difficulty of forming fast and effective memory associations with faces, combined with the face locations being shuffled at each attempt (though our methodology does not illustrate which aspect is the most significant).

PressurePIN was successfully observed by 2 of observers (14%), which is a significant improvement over a PIN in its traditional form. These observers commented that their strategy was to focus attention on one hand per observation, and use the third observation to validate the information obtained. PressureFaces was not successfully compromised by any observer. This led us to analyze the extent to which components of authentication sequences were recalled (i.e. how many of the 4 faces, or 4 digits, each observer correctly identified). Table 3 shows the accuracy of participants per system. Although observers were able to select one correct component of a PressureFaces sequence in 40% of attempts, we can attribute this to random guessing ($\frac{4}{9} = 44.4\%$), particularly given that all observers claimed to have no knowledge of any face components when questioned after the experiment.

In addition to observer success rates, we recorded the login durations for the designated *inputters*. From this we hoped to gain an impression as to how the Pressure-Grid impacted user performance, as has been discovered in numerous other mechanisms designed to be resistant to shoulder surfing. We did not analyze timings for observers as we did not specify timing to them as a specific concern. These login times were subject to a 2 (PIN vs. faces) × 2 (pressure vs. no pressure) analysis of variance using SPSS that demonstrated significant main effects on both factors, with PIN logins proving faster than faces ($F(1, 20) = 61.89, p < 0.001$), and pressure systems proving slower than no-pressure systems ($((1, 20) = 234.51, p < 0.001$). There was no significant interaction between conditions. The distribution of login times for each of the four conditions are illustrated in Figure 9.

After the experiment we asked participants to complete a short questionnaire to elicit opinions on each of the systems and the problem domain. Overall participants were experienced with multi-touch interfaces with 66% having previously used one. 72% were concerned about the ease of observing passwords and PINs entry in everyday life, and 50% of participants reported no confidence in the privacy of their PIN when entered in public environments. When asked about perceived usability of Pressure-Grid, 67% of users scored this at 4/5 and above, also 78% rated the privacy offered by the Pressure-Grid at 5/5.

DISCUSSION

With a relatively small sample size, the user study results confirmed our hypothesis that Pressure-Grid would be a significant defense against shoulder surfing for PIN and graphical password systems on tabletop interfaces. One surprising aspect was that observers were able to compromise the PressurePIN when the location of the numeric digits was static between logins. During the user study we became aware of a collaborative attack on PressurePIN, where two observers could collude to observe the workings of one hand each, and later combine the information. During informal discussions with participants, many considered this to be a realistic threat, particularly those who had already developed a successful strategy against PressurePIN. The results of the PressureFaces system demonstrate that this vulnerability can be secured by randomizing PIN digit locations since no participants were able to compromise this randomized configuration. This would most likely increase the average login duration, but we suspect this would not be greater than the average duration of a PressureFaces login of 10.8 seconds. In terms of overall login durations the Pressure-Grid performs favorably in comparison to a number of other authentication mechanisms with similar goals. The addition of Pressure-Grid added approximately three seconds to the average login duration of both PIN and Faces.

The results must also force a reconsideration of a common assumption that graphical passwords are more vulnerable to shoulder surfing than PINs and alphanumeric passwords. In our study, without the Pressure-Grid 50% more participants were able to successfully observe and re-enter a PIN over our Faces system. This is also despite the reduced entropy of Faces vs. PIN (9^4 vs. 10^4). This could suggest the greater difficulty of forming a fast visual memory encoding, and a memorable verbal encoding in the form of a description [7]. This complicates retention for an observer who has limited time to retain images. The study by Tari et. al. [28] discovered that 5 character passwords (not comprising meaningful words) were more vulnerable to observation than a sequence of 5 Passfaces selected with mouse input – although the difference was not large. More research with greater numbers of participants is required to firstly prove or disprove this effect, and also determine whether it is unique to faces, or extends to other images too.

Recreating a spontaneous phenomenon such as shoulder surfing in a laboratory presents significant experimental design challenges, and is certain to attract questions of ecological validity. In a laboratory the participants are aware of the artificial scenario, and because of the socially intrusive task being performed it is a risk that their resulting actions are not representative of real world use. Especially due to the fact that etiquette and typical user behavior in these scenarios is not yet widely known. We cannot claim to have perfectly re-created the phenomenon; however, our goal was to create a scenario to facilitate analysis of the observation resistance provided by each system. The best insight can potentially be gained by passively evaluating the mechanisms *in situ*.

Considering all system designs, we believe ShieldPIN, CuePIN, and Pressure-Grid to be promising exemplars of authentication on multi-touch interfaces. Further research and development is needed to make CuePIN and Pressure-Grid suitable for real installations, however ShieldPIN offers a number of instant benefits. Firstly it is based on the existing PIN entry paradigm which makes it likely to be intuitive to diverse groups of users; its limitations can be easily perceived by users; and finally its simple design makes it highly deployable.

FINAL REMARKS

The results obtained give rise to a number of other operational considerations. Firstly, most shared interfaces are not capable of distinguishing the identity of users, and so a further challenge concerns how to ensure that authenticated access to an object remains restricted to a particular user throughout a session. A simple software response to the problem could be to restrict the movement of authenticated objects beyond protected areas of the surface. A more elaborate solution could integrate a floating *authentication lens* analogous to Magic Lenses [2] that can be dragged with the non-dominant hand using a finger or a tangible object recognized by the system. Once the user has authenticated the lens could disclose information and functions beneath the lens that the user is authorized to view and access. Our future work will focus on this and new interface paradigms for enforcement of privacy and security policies that exploit directly mapped interactions afforded by multi-touch displays.

ACKNOWLEDGMENTS

This work was supported in part by Microsoft Research through its PhD Scholarship Programme, the Engineering And Physical Science Research Council (EPSRC), and One North East.

REFERENCES

1. D. Baker. Nondisclosing password entry system. U.S. Patent 5,428,349 June 27, 1995.
2. E. A. Bier, M. C. Stone, K. Pier, K. Fishkin, T. Baudel, M. Conway, W. Buxton, and T. DeRose. Toolglass and magic lenses: the see-through interface. In *CHI '94: Conference companion on Human factors in computing systems*, pages 445–446, New York, NY, USA, 1994. ACM.
3. S. Brostoff and M. A. Sasse. Are passfaces more usable than passwords? a field trial investigation. In *Proceedings of HCI 2000*, 2000.
4. L.-W. Chan, T.-T. Hu, J.-Y. Lin, Y.-P. Hung, and J. Hsu. On top of tabletop: A virtual touch panel display. In *Horizontal Interactive Human Computer Systems, 2008. TABLETOP 2008. 3rd IEEE International Workshop on*, pages 169–176, Oct. 2008.
5. A. De Luca and B. Frauendienst. A privacy-respectful input method for public terminals. In *NordiCHI '08: Proceedings of the 5th Nordic conference on Human-computer interaction*, pages 455–458, New York, NY, USA, 2008. ACM.
6. A. De Luca, E. von Zezschwitz, and H. Hussmann. Vibrapass - secure authentication based on shared lies. In *27th ACM SIGCHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2009.
7. P. Dunphy, J. Nicholson, and P. Olivier. Securing passfaces for description. In *SOUPS '08: Proceedings*

of the 4th symposium on Usable privacy and security, pages 24–35, New York, NY, USA, 2008. ACM.

8. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The design and analysis of graphical passwords. In *SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium*, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

9. B. Malek, M. Orozco, and A. E. Saddik. Novel shoulder-surfing resistant haptic-based graphical password. In *EuroHaptics 2006*, pages 179–184, jul 2006.

10. J. Marshall, T. Pridmore, M. Pound, S. Benford, and B. Koleva. Pressing the flesh: Sensing multiple touch and finger pressure on arbitrary surfaces. In *Pervasive Computing*, Lecture Notes in Computer Science, pages 38–55. Springer, May 2008.

11. M. J. Martino, G. L. Meissner, and R. C. J. Paulsen. Identity verification system resistant to compromise by observation of its use. U.S. Patent 5,276,314 January 4, 1994.

12. Microsoft Surface. http://www.surface.com.

13. K. D. Mitnick and W. L. Simon. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc., New York, NY, USA, 2003.

14. Passfaces Corporation. http://www.passfaces.com.

15. T. Pering, M. Sundar, J. Light, and R. Want. Photographic authentication through untrusted terminals. *IEEE Pervasive Computing*, 2(1):30–36, 2003.

16. V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 236–245, New York, NY, USA, 2004. ACM.

17. S. Sakurai, Y. KItamura, S. Subramanian, and F. Kishino. Visibility control using revolving polarizer. In *Horizontal Interactive Human Computer Systems, 2008. TABLETOP 2008*, pages 161–168. IEEE, October 2008.

18. H. Sasamoto, N. Christin, and E. Hayashi. Undercover: authentication usable in front of prying eyes. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 183–192, New York, NY, USA, 2008. ACM.

19. J. Schöning, P. Brandl, F. Daiber, F. Echtler, O. Hilliges, J. Hook, M. Löchtefeld, N. Motamedi, L. Muller, P. Olivier, T. Roth, and U. von Zadow. Multi-touch surfaces: A technical guide. techreport, 2008.

20. J. Schöning, M. Rohs, and A. Krüger. Spatial authentication on large interactive multi-touch surfaces. In *IEEE Tabetop 2008: Adjunct Proceedings of IEEE Tabletops and Interactie Surfaces*, October 2008.

21. G. B. D. Shoemaker and K. M. Inkpen. Single display privacyware: augmenting public displays with private information. In *CHI '01: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 522–529, New York, NY, USA, 2001. ACM.

22. P. Sinha, B. Balas, Y. Ostrovsky, and R. Russell. Face recognition by humans: Nineteen results all computer vision researchers should know about. *Proceedings of the IEEE*, 94(11):1948–1962, January 2007.

23. R. T. Smith and W. Piekarski. Public and private workspaces on tabletop displays. In *AUIC '08: Proceedings of the ninth conference on Australasian user interface*, pages 51–54, Darlinghurst, Australia, Australia, 2008. Australian Computer Society, Inc.

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

25. X. Suo, Y. Zhu, and G. S. Owen. Graphical Passwords: A Survey. In *ACSAC '05: Proceedings of the 21st Annual Computer Security Applications Conference*, pages 463–472, Washington, DC, USA, 2005. IEEE Computer Society.

26. T. Takada, T. Onuki, and H. Koike. Awase-e: Recognition-based image authentication scheme using users' personal photographs. In *Innovations in Information Technology, 2006*, pages 1–5, Nov. 2006.

27. D. S. Tan, P. Keyani, and M. Czerwinski. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *OZCHI '05: Proceedings of the 17th Australia conference on Computer-Human Interaction*, pages 1–10, Narrabundah, Australia, Australia, 2005. Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

28. F. Tari, A. A. Ozok, and S. H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 56–66, New York, NY, USA, 2006. ACM.

29. D. Vogel and R. Balakrishnan. Interactive public ambient displays: transitioning from implicit to explicit, public to personal, interaction with multiple users. In *UIST '04: Proceedings of the 17th annual ACM symposium on User interface software and technology*, pages 137–146, New York, NY, USA, 2004. ACM.

30. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *AVI '06: Proceedings of the working conference on Advanced visual interfaces*, pages 177–184, New York, NY, USA, 2006. ACM.

31. M. Wu and R. Balakrishnan. Multi-finger and whole hand gestural interaction techniques for multi-user tabletop displays. In *UIST '03: Proceedings of the 16th annual ACM symposium on User interface software and technology*, pages 193–202, New York, NY, USA, 2003. ACM.