BoD Taps: An Improved Back-of-Device Authentication Technique on Smartphones

Luis A. Leiva*
PRHLT Research Center
Universitat Politècnica de València
luileito@prhlt.upv.es

Alejandro Catalá
ISSI-DSIC
Universitat Politècnica de València
acatala@dsic.upv.es

ABSTRACT

Previous work in the literature has shown that back-of-device (BoD) authentication is significantly more secure than standard front-facing approaches. However, the only BoD method available to date (*BoD Shapes*) is difficult to perform, especially with one hand. In this paper we propose *BoD Taps*, a novel approach that simplifies BoD authentication while improving its usage. A controlled evaluation with 12 users revealed that *BoD Taps* and *BoD Shapes* perform equally good at unlocking the device, but *BoD Taps* allows users to enter passwords about twice faster than *BoD Shapes*. Moreover, *BoD Taps* is perceived as being more usable and less frustrating than *BoD Shapes*, either using one or two hands.

Author Keywords

Back of device interaction; Unlocking; Passwords

ACM Classification Keywords

H.5.2 User Interfaces: Input devices and strategies; K.6.5 Security and Protection: Authentication

INTRODUCTION

There is an increasing need to improve protection in mobile devices due to the sensitive data that they give access to, e.g., private chats or online banking. If a smartphone is stolen or accidentally lost, it is important for its owner to gain enough time so that he can use a computer and lock the SIM, deactivate online accounts, or even wipe the device remotely. In this regard, we are particularly interested in exploring the authentication problem, or that of verifying that the user is the one trying to access his device.

A common approach to authenticating a user consists in locking the device so that a *secret* (e.g., a code or password) has to be entered to unlock it. Typical methods to this end are PINs (numerical passwords) or Gridlocks (drawing patterns that connect predefined dots). However, given the frequency of unlocking actions in public or shared spaces, shoulder surfing [12] and smudge attacks [1] could become a threat.

*Authorship determined by coin tossing.

MobileHCI 2014, September 23–26, 2014, Toronto, ON, Canada.

ACM 978-1-4503-3004-6/14/09 ...$15.00.
http://dx.doi.org/10.1145/2628363.2628372

With these two issues in mind, De Luca *et al.* [8] explored the use of Back of Device (BoD) interaction and designed *BoD Shapes*, a pattern-based BoD authentication method that uses relative movements to describe shapes consisting of combinations of horizontal and vertical strokes. It was found that such method provides better security features against shoulder surfing attacks, for which "average" curious people will have it harder to authenticate. Unfortunately, the method presents some weaknesses. For instance, having to slide the finger to describe horizontal and vertical strokes can be difficult to perform due to the anatomy of the human finger, which is especially true for describing corner strokes with the same hand that grabs the device. In fact, as stated by their authors, *BoD Shapes* seemed to be not usable with one hand.

These observations made us wonder if it would be still possible to provide an acceptable alternative to BoD authentication. We believe that a method that supports one-handed BoD authentication would be of particular importance, as the second hand is often occupied with a primary or secondary task [9]. Moreover, as authentication is occurring very often in our daily lives, it is important that the process can be executed fast and effortless.

This paper presents *BoD Taps*, a novel BoD authentication method that is highly usable and theoretically more secure than *BoD Shapes*. We found that users can successfully unlock their smartphones with *BoD Taps*, either with one hand or two hands, as indicated by usability and cognitive effort indicators. We also found that *BoD Taps* allows users to create and enter passwords about twice faster than *BoD Shapes*.

RELATED WORK

Common unlock methods shipped in current mobile devices include Slide, PIN, Password, Face or Voice Unlock, and Pattern (also known as Gridlock). These methods are simple and effective, though they are susceptible to observation attacks. In the research literature we can find a number of alternatives to make devices less susceptible to shoulder surfing. For instance, drawing geometric shapes over a dial pad [13], using tactile cues to obfuscate a PIN entry [7], multi-touch braille-like input [2], or a sequence of user-generated pictures [11]. More esoteric approaches include rotating dials [4] and virtual wheels [3], accelerometer-based gestures [10], or keystroke analysis [6].

Ultimately, preventing shoulder surfing attacks is difficult as long as authentication takes place at the front of the device [8]. A possible alternative would be using biometric-based methods, such as iPhone's Touch ID, however to date

the iPhone is the only mobile device that has a fingerprint reader. Moreover, people may have privacy concerns. This is especially true when providing biometric data to service providers or employers [13]. We believe that moving authentication to the back of the device is a compromise solution worth exploring. In fact, some mobile devices already have BoD touch capabilities like the Playstation Vita or the Docomo F-04D smartphone, thus it is likely that this topic will be appealing in the near future.

METHOD DESCRIPTION

A fundamental design consideration is that of unintentional interaction at the beginning of the authentication process. Indeed, De Luca *et al.* [8] detected accidental BoD strokes before users actually meant to start entering a password. We thus considered an activation gesture (a long tap, circa 1 second) to indicate that a password will be entered. This way, spurious touches and movements while grasping the device are easily ignored. Also, an advantage of the long tap gesture is the possibility to include several fingers for activation, so that the number of fingers involved in the process matters.

With the aim of making the BoD authentication process easier to use, we considered tap contacts as main primitives for the design of *BoD Taps*. This decision should address some of the difficulties presented by *BoD Shapes*, such as the need to describe corners, allowing users to unlock their devices more comfortably; see Figure 1.

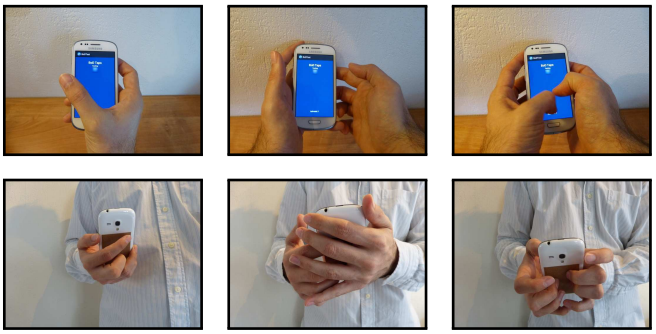

Figure 1: Different ways of interacting with *BoD Taps*, simulating a BoD-capable device. Top row: shoulder surfer view. Bottom row: front view.

The underlying password in *BoD Taps* consists of the number of activation fingers plus a sequence of tokens after activation. Each token is a tap described by relative positions of the fingers according to a 9-directional code. This code considers the typical eight directions (L=Left, U=Up, R=Right, D=Down, LU=Left-Up,...) along with a neutral position (N=Neutral) that represents the same position of the previous token in the sequence. Figure 2 illustrates the kind of codes that are defined in *BoD Taps* and *BoD Shapes*. We should remark that in *BoD Taps* several fingers can be involved in the process, both before and after activation, and so the number of touching fingers are advantageously taken into account. This should in turn help making passwords more resilient against shoulder surfer attacks.

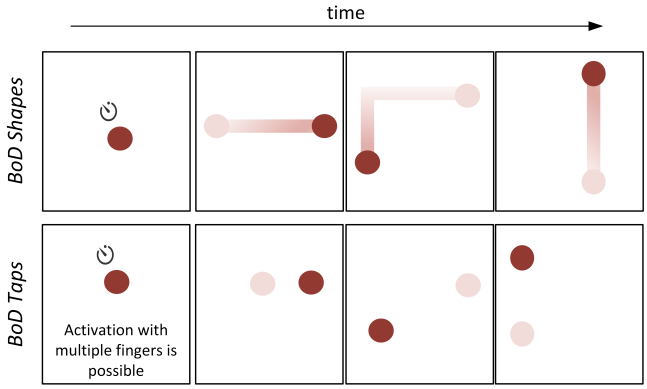

Figure 2: One-finger conceptual comparison. In *BoD Shapes* this password would be encoded as `"1.R.LD.U"` while in *BoD Taps* it would be encoded as `"1.1R.1LD.1U"`.

Theoretical Security Analysis

Information entropy is a common measure of password strength, indicating how robust a technique is to guessing or brute-force attacks [5]. In this metric, the information entropy of a password of n symbols from a symbol set of size m is $\log_2 m^n$, measured in bits. In other words, the information entropy of a password technique is the minimum number of bits needed to encode the set of all possible passwords, assuming all symbols are equally likely [2].

In one *BoD Taps* token there are $3 \times 2 \times 9$ possible combinations: one finger is always touching, but up to 3 fingers can be either touching or not and 9 relative positions are available for each finger. Therefore, a password with 3 tokens has information entropy of $\log_2(54^3) = 17.2$ bits. Moreover, if two hands are used entropy increases more than twice, given all possible combinations regarding the number of fingers involved. By contrast, one *BoD Shapes* token can have up to 3 strokes, where each stroke can be performed in 4 directions and two consecutive strokes cannot have the same direction, making a total of 36 possibilities. Therefore a *BoD Shapes* password with 3 tokens has information entropy of $\log_2(36^3) = 15.5$ bits. Now consider the information entropy of a 4-digit PIN. Each digit has 10 possible inputs, so the PIN has $\log_2(10^4) = 13.2$ bits of information entropy. In sum, the information entropy of *BoD Taps* is higher, indicating that it is theoretically stronger.

USER STUDY

We ran a controlled experiment using BoD unlock tests with both one hand and two hands. The main goal was to evaluate the feasibility of *BoD Taps* as well as comparing it against *BoD Shapes*, its closest peer. Four hypotheses were stated:

1. *BoD Taps* is less error-prone than *BoD Shapes*.
2. *BoD Taps* is faster to perform than *BoD Shapes*.
3. *BoD Taps* is more usable than *BoD Shapes*.
4. *BoD Taps* is less frustrating than *BoD Shapes*.

Apparatus

We used a Google Nexus 4 (4.7” screen, 1280x768 px at 320 ppi) running Android 4.4.2 (KitKat). Using the same smart-

phone for all participants eliminates the effect of device and the effect of screen size. Moreover, this is a very light device (140 g of weight) so it can simulate a BoD-capable device by placing the touchscreen face down to enable BoD interaction. We put a sticker in the rear side to simulate the front of the phone (Figure 3b). Rubber bands were attached to the edges of the screen to avoid palm interactions (Figure 3a).

(a) (b) (c)

Figure 3: Experimental BoD phone setup (3a, 3b) and screenshot of the acquisition tool (3c).

The Android app we used for gathering data (Figure 3c) featured a practice mode, so that participants could try different methods and hand poses before entering the actual record mode. Since the screen of the smartphone would not be visible to participants, we included haptic response through vibration on touch events and different audio cues—one sound for each type of "key event", e.g., system activated, password entered, successful/unsuccessful unlocks.

Participants

We recruited 12 right-handed participants (4 female) aged 21–35 (M=26.3, SD=2.1) using our University's mailing lists. Participants were either university staff or students, with no technical background in security or privacy topics. The unlock methods they use were PIN (3 participants), slide (4), grid (4), and none (1). When asked about their unlock choice, the most common agreement was *"because it is fast and easy to perform."* People stated that they use to unlock their devices about 30 times a day (M=29.5, SD=11.7), either with one hand (5 participants), two hands (3), or both (4).

Design

We considered two independent factors with 2 levels each: *Method* (shapes or taps) and *Pose* (1 or 2 hands). We measured authentication attempts and errors, speed of password creation and execution, and usability plus work load. We used a repeated measures within-subjects design, i.e., participants were assigned to all treatment levels. We used Latin squares to counterbalance the order of the conditions and reduce learning effects. For the statistical analysis, data were accumulated for each participant and were analyzed with the two-way ANOVA test (data met the required test conditions).

Procedure

To begin, we briefly described the purpose of the study. Participants signed in a consent form followed by a demographics questionnaire. Then, both authentication techniques were demoed front-of-device with one and two hands, respectively. After each demo, participants were asked to try themselves on the simulated BoD device (Figure 3). Next, the actual evaluation began. All interactions were performed at the back, as the touchscreen was facing down (Figure 3b).

Each participant was told to define up to 3 self-selected BoD passwords (*record* mode) under the 4 conditions, so that each participant would perform at least 12 BoD unlock tests overall. Once each password was defined, the following distraction task was used. The evaluator grabbed the phone and put the app in *test* mode, then the phone was given back to the participant, with the touchscreen facing down, who had to re-enter the BoD password. As in commercial smartphones or ATMs, participants could retry up to 3 times. When each condition was finished, participants were asked to answer the SUS and NASA-TLX questionnaires on a nearby laptop.

Results

Participants were mostly successful at unlocking the device (Table 1). ANOVA revealed no significant differences regarding *Method* and *Pose* ($p > .05$), and no significant *Method*Pose* interaction was found, suggesting that both authentication methods are comparable under the tested conditions. Therefore, our first hypothesis was rejected.

	1 hand		2 hands	
Method	**Attempts**	**Successful**	**Attempts**	**Successful**
BoD Shapes	2.25 (0.8)	74.9%	2.83 (0.5)	94.4%
BoD Taps	2.41 (1.0)	80.5%	2.08 (0.9)	69.4%

Table 1: Mean (and SD) number of unlock attempts and overall authentication success rate.

To fairly test our second hypothesis, i.e., password entry speed (Table 2), we considered the *effective* time, i.e., the time required to enter each password after activation. Both methods used the same long tap gesture (1 s) for activation.

Regarding password creation speed, we found that *BoD Taps* allows users to define and enter passwords nearly twice faster than *BoD Shapes*. However, no significant differences were found regarding *Method* and *Pose*, and no significant *Method*Pose* interaction was found. This reveals that participants invested a comparable amount of time defining their own passwords under the tested conditions.

Regarding authentication speed, significant differences were found between *Method* [$F_{1,44} = 10.367, p = .002, \eta_p^2 = 24.12$] but not in terms of *Pose*. No significant *Method*Pose* interaction was found. No pairwise comparisons were performed because each factor has only two levels. Therefore, our second hypothesis was thus partially verified, i.e., users entered BoD passwords with *BoD Taps* faster that *BoD Shapes* just in terms of authentication speed.

On the other hand, participants preferred *BoD Taps* over *BoD Shapes* both in terms of usability and task load (Table 3). ANOVA revealed that differences were significant regarding *Method* [SUS: $F_{1,44} = 13.062, p < .001, \eta_p^2 = 2.25$;

	Creation speed		Authentication speed	
Method	**1 hand**	**2 hands**	**1 hand**	**2 hands**
BoD Shapes	5.5 (0.5)	5.1 (0.4)	3.4 (0.2)	4.0 (0.3)
BoD Taps	4.4 (0.9)	3.7 (0.2)	2.1 (0.1)	2.6 (0.2)

Table 2: Mean (and SD) password entry speed, in seconds.

TLX: $F_{1,44} = 13.874, p < .001, \eta_p^2 = 1.61$] and *Pose* [SUS: $F_{1,44} = 5.806, p = .020, \eta_p^2 = 1$; TLX: $F_{1,44} = 8.581, p < .01, \eta_p^2 = 1$]. A significant *Method*Pose* interaction effects was found in terms of SUS [$F_{1,44} = 4.483, p = .039, \eta_p^2 = 0.77$] but not in terms of TLX. No pairwise comparisons were performed because each factor has only two levels. Therefore, our third and fourth hypotheses were both verified, i.e., *BoD Taps* was significantly perceived as being more usable and less frustrating than *BoD Shapes*.

	SUS score		TLX score	
Method	**1 hand**	**2 hands**	**1 hand**	**2 hands**
BoD Shapes	47.7 (29.2)	73.5 (18.7)	5.6 (1.3)	4.2 (1.1)
BoD Taps	80.4 (14.3)	82.1 (12.2)	3.9 (1.1)	3.4 (0.7)

Table 3: Mean (and SD) usability scores (SUS $\in [0, 100]$, higher is better) and work load scores (TLX $\in [0, 100]$, lower is better).

DISCUSSION AND CONCLUSIONS

It is worth pointing out that both BoD authentication methods were new to all participants. Still, evaluation results were quite good. Especially for one-handed authentication, the smartphone's form factor proved to be a burden for the participants using *BoD Shapes*. However, for *BoD Taps* it did not seem to be the case.

We performed an additional analysis on the effect of diagonal *BoD Taps* on authentication errors. In 51% of the one-handed trials and 58% of the two-handed trials the error was due to a difference of at least 1 token between created and entered password; c.f., `"2.1D.2R.1D"` vs. `"2.1D.2R.1DL"`. These results suggest that ignoring diagonal taps should improve accuracy and make *BoD Taps* work better in practice. Further, users commented that they took riskier decisions while defining their own passwords with *BoD Taps*, often when using both hands. This may explain the fact that users performed more successful unlocks using *BoD Taps* with one hand than with two hands.

One user commented that *"I personally was having trouble making corner-like shapes. Hence the shapes I defined were very simple, mostly straight lines."* A deeper analysis of all user-defined passwords, using the mean string distance (MSD) over all password combinations, revealed that there were consistently more variability in those created with *BoD Taps* [$\text{MSD}_{1\text{hand}}$ = 5.85, *SD*=3.1; $\text{MSD}_{2\text{hands}}$ = 6.62, *SD*=3.0] than in those created with *BoD Shapes* [$\text{MSD}_{1\text{hand}}$ = 3.46, *SD*=1.9; $\text{MSD}_{2\text{hands}}$ = 4.98, *SD*=3.2]. This suggests not only that participants were more creative using *BoD Taps*, but also that users defined simpler *BoD Shapes* passwords apparently to increase their usability and performance.

Participants also commented that unlocking the device with two hands provides more password choices, which in turn allows for defining more complex token combinations. This was mentioned for both authentication methods and is in fact corroborated by the aforementioned MSD computations. Finally, we acknowledge that further analysis should be conducted with a larger sample size, possibly in the wild, in order to draw definitive conclusions. All in all, it is our hope that this work will provide designers and researchers with a new understanding of BoD authentication methods.

ACKNOWLEDGMENTS

We thank Alexander De Luca, Alireza Sahami, Niels Henze, and Albrecht Schmidt for fruitful discussions. We also thank the anonymous MobileHCI reviewers for providing suggestions to strengthen this paper. Work supported by the EU FP7 program (grant 600707), GVA VALi+d program (grant APOSTD/2013/013), and MINECO (grant TIN2010-20488).

REFERENCES

1. Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. In *Proc. USENIX WOOT* (2010), 1–7.
2. Azenkot, S., Rector, K., Ladner, R., and Wobbrock, J. Passchords: secure multi-touch authentication for blind people. In *Proc. ASSETS* (2012), 159–166.
3. Bianchi, A., Oakley, I., Kostakos, V., and Kwon, D. S. The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In *Proc. TEI* (2011).
4. Bianchi, A., Oakley, I., and Kwon, D. Spinlock: A single-cue haptic and audio PIN input technique for authentication. In *Proc. Haptic and Audio Interaction Design* (2011), 81–90.
5. Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S., and Nabbus, E. A. Electronic authentication guideline. NIST Special Publication 800-63-1, 2011.
6. Clarke, N., and Furnell, S. Authenticating mobile phone users using keystroke analysis. *Intl. J. of Inf. Security 6*, 1 (2007), 1–14.
7. De Luca, A., von Zezschwitz, E., and Hussmann, H. Vibrapass: secure authentication based on shared lies. In *Proc. CHI* (2009), 913–916.
8. De Luca, A., von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scipioni, M. P., and Langheinrich, M. Back-of-device authentication on smartphones. In *Proc. CHI* (2013), 2389–2398.
9. Hirotaka, N. Reassessing current cell phone designs: using thumb input effectively. In *Proc. CHI EA* (2003), 938–939.
10. Patel, S. N., Pierce, J. S., and Abowd, G. D. A gesture-based authentication scheme for untrusted public terminals. In *Proc. UIST* (2004), 157–160.
11. Takada, T., and Koike, H. Awase-e: Image-based authentication for mobile phones using user's favorite images. In *Proc. MHCI* (2003), 347–351.
12. Tari, F., Ozok, A. A., and Holden, S. H. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proc. SOUPS* (2006), 56–66.
13. Weiss, R., and De Luca, A. Passshapes - utilizing stroke based authentication to increase password memorability. In *Proc. NordiCHI* (2008), 383–392.