Bu-Dash: A Universal and Dynamic Graphical Password Scheme

Panagiotis Andriotis[1,2][0000−0002−3490−3123], Myles Kirby[1], and Atsuhiro Takasu[2][0000−0002−9061−7949]

[1] University of the West of England, Bristol, BS16 1QY, U.K.
panagiotis.andriotis@uwe.ac.uk
[2] National Institute of Informatics, Tokyo, 101-8430. Japan

Abstract. Biometric authentication gradually replaces knowledge-based methods on mobile devices. However, Personal Identification Numbers, passcodes, and graphical password schemes such as the Android Pattern Unlock (APU) are often the primary means for authentication, or they constitute an auxiliary (or backup) method to be used in case biometrics fail. Passcodes need to be memorable to be usable, hence users tend to choose easy to guess passwords, compromising security. The APU is a great example of a popular and usable graphical password scheme which can be easily compromised, by exploiting common and predominant human behavioristic traits. Despite its vulnerabilities, the scheme's popularity has led researchers to propose adjustments and variations that enhance security but maintain its familiar user interface. Nevertheless, prior work demonstrated that improving security while preserving usability remains frequently a hard task. In this paper we propose a novel graphical password scheme built on the foundations of the well-accepted APU method, which is usable, inclusive, universal, and robust against shoulder surfing and smudge attacks. Our scheme, named `Bu-Dash`, features a dynamic user interface that mutates every time a user swipes the screen. Our pilot studies illustrate that `Bu-Dash` attracts positive user acceptance rates and maintains acceptable usability levels.

Keywords: Smudge Attacks · Android Pattern · User Authentication · Shoulder Surfing.

1 Introduction

User authentication on mobile devices is a ubiquitous task performed daily by millions of users. Personal Identification Numbers (PIN) have been widely used during mobile computing's adolescence, but after 2010 we have seen a remarkable variety of proposals that aim to replace 4- or 6-digit PIN screen lock methodologies (alphanumeric, graphical, biometrics, implicit authentication). Android developers were among the first that attempted to introduce a graphical-based method for user authentication on mobile devices proposing the APU scheme during 2008 [13]. Earlier studies have shown that the APU is still utilized by at least 25% of Android users [13, 24].

The proliferation of biometric methods is evident nowadays due to the increased usability they offer, urging users to replace traditional text or graphical passwords (knowledge-based) with fingerprint and face identification methods [36] (biometric-based). However, although biometrics seems to be the preferred user authentication methodology, there still exists the need to set up a secondary password on the device in case the biometric sensor fails. Therefore, text or graphical-based passcodes are still necessary to ensure smooth and untroubled authentication for mobile device users.

Prior work on text-based authentication investigated the transition from 4- to 6-digit PIN passcodes and concluded that longer PINs attain only marginally improved security [32]. The transition from 4-digit to longer passcodes was the only notable security upgrade of this knowledge-based user authentication method for mobile devices. On the other hand, several graphical password schemes have been proposed aiming to provide more usable and secure solutions for mobile devices [14, 17, 34].

Focusing particularly on the APU, the addition of password meters as an improvement towards raising users' security awareness has been studied extensively [2, 27, 28], but such solutions have not been considered yet for inclusion by the industry. In addition, research has shown that similarly to the extension of the 4- digit to 6-digit format for passcodes [24], strategies like the expansion from the standard 3x3 to a 4x4 grid, do not offer significant security enhancements [4]. Other proposals include node re-arrangement [29], system-guided contact point selection [9], or dual super-imposed input on the same 3x3 grid [13] aiming to prevent or minimize threats from shoulder surfing attacks. The common characteristic of these methods is their intention to propose (mainly minor) structural interventions to the original APU scheme that will not drastically affect users' familiarity with the interface, avoiding users' frustration and disapproval.

Despite the plethora of proposals to improve graphical passwords against smudge [6] and shoulder surfing attacks [16], to the best of our knowledge, there is no research work that attempts to assess the feasibility of using a methodology which is based on the implementation of a dynamic grid. In this paper we introduce Bu-Dash, a proof of concept based on design principles found in the APU and in gaming platforms[3].

Initially inspired from the *Morse code* and its use of dots (or Bullet points ●) and Dashes (–) to create an encoded vocabulary/lexicon to be used in telecommunications, we envisioned a passcode scheme that comprises shapes/symbols instead of alphanumerical characters. However, because the use of only two symbols in a password would introduce security issues (i.e., limited password space), we propose to utilize additional symbols as the passcodes' potential building blocks: ○, □, -, △, ×. These shapes should probably look familiar to gamers[4], or other broader audiences[5]. Their selection was based on research which demon-

[3] https://www.playstation.com/en-gb/legal/copyright-and-trademark-notice/

[4] We utilized Google's "Material Icons" as the password building blocks in this research work: https://fonts.google.com/icons

[5] We refer to viewers of the popular series "Squid Game".

strates that these are the least complex shapes in a series of different candidates [10].

Additionally, to defend from shoulder surfing and mainly smudge attacks, we propose a novel approach in designing graphical password schemes. Instead of forming the password by swiping a finger on the nodes of a static grid, we propose the use of a dynamically changing grid. `Bu-Dash` is based on the popular APU 3x3 node interface which is well-known to mobile device users. However, instead of having static nodes (i.e., ●), `Bu-Dash`'s grid is dynamic, featuring randomly assigned shapes in its nodes (○, □, -, △, ×). The shapes keep changing every time users move their fingers on the grid making the scheme more robust to shoulder surfing and smudge attacks, without drastically affecting its usability. In summary, this paper makes the following contributions:

- We propose a novel graphical password scheme based on Android's popular 3x3 node interface that is secure against smudge attacks.
- We develop a mobile application to showcase the `Bu-Dash` system and collect preliminary feedback from mobile device users.
- We conduct a series of pilot studies with users who volunteered to participate and comment on the feasibility of introducing such a scheme.
- We report early results that show usability is not drastically reduced due to the introduction of a shifting grid on the scheme's interface.

2 Related Work

Graphical passwords for mobile devices have been introduced as a more usable solution for user authentication because graphical information is more memorable by humans [11]. Prior work on Android patterns however investigated users' biases and habits when interacting with the 3x3 node interface and found favorable starting/ending points and N-grams [3], which are sometimes related to the influence of human factors such as users' handedness [1]. The APU security was quantified by Uellenbeck et al. [30] who found that, in theory, APU selection is as diverse as selecting a 3-PIN password [13]. The lack of APU's passcode diversity due to human aspects was also confirmed by Aviv et al. [4] in an online study, and more extensively by Loge et at. [23] whose work showcased users' poor security perceptions when forming passcodes in different contexts (e.g., authentication in banking or shopping apps). The APU has been also studied as an attack surface with research focusing basically on side channel and guessing attacks. Aviv et al. [6] showed that smudges (unintentionally residing on mobile devices' screens) can eventually aid guessing attacks against users' passwords. Andriotis et al. [3] combined insights retrieved from collected passcodes and performed an *in situ* lab study, experimenting with guessing attacks. At a later work, they commented on the feasibility of performing successful guessing attacks on the APU using common knowledge [1]. Android patterns are also susceptible to shoulder surfing [5] and video-based attacks [33]. However, the APU scheme remains popular among Android users [24] drawing researchers' attention.

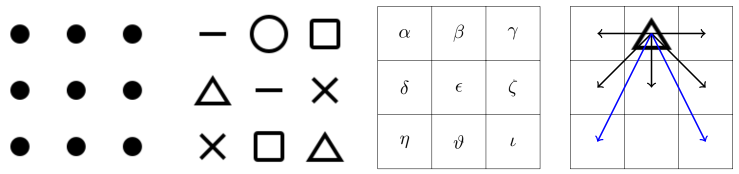
The lack of diversity in choosing Android patterns and the influence of human biases in the scheme's security have led researchers to propose a variety of solutions aiming to make the APU more robust to smudge attacks [15, 20, 26] and shoulder surfing [12]. Another strand of research proposes the use of password meters to diversify input and enhance awareness [2, 27, 28]. Other proposals incorporate dual input on the same 3x3 framework [13], feature extended 4x4 grid interfaces [4], utilize background images and animations to enhance passcode selection [35], employ assisted pattern formation [9], or integrate blocklists [25] to enable a more diverse pattern selection and incommode guessing attacks. Most of these solutions do not alter radically the well-known 3x3 interface, but they attempt to include small adjustments in the user authentication experience keeping the main grid in a static state. Tupsamudre et al. [29] propose an alternate circular layout (namely "Pass-O") simplifying the APU drawing rules. Their usability evaluation shows that users tend to create shorter and less complex passwords under the Pass-O scheme [31].

Alternative layouts and dynamic grids have been proposed in the past for *PIN-based* authentication aiming to minimize the influence of shoulder surfing attacks. However, floating [17] or rotating [8] grids result in longer login times than conventional text-based systems, and gesture-based proposals such as "SwiPIN" [34] might require long training periods for the user to become familiar with. Other proposals include the use of colors and shapes in the user authentication process. "Chameleon" is a hybrid scheme using a mixture of digits, colors and shapes but it is not clear whether it can fit in small screens like these used on smartphones [18]. Some of the shapes used in this work (○, □, △) are similar to those we utilize for the Bu-Dash scheme. Similar symbols with the ones we use in our paper are also incorporated in Lee's work [22]. Finally, similar to our scheme, " SteganoPIN" [21] and " SwitchPIN" [19] are using dynamic interfaces that randomly assign digits on 3x3 grids. The SteganoPIN creators however state that their system is more appropriate for ATM and PoS systems rather than mobile devices.

In this paper we propose Bu-Dash, the first graphical password scheme for mobile devices that adopts concepts from aforementioned work, but aims to present a more usable and simple authentication process. We assume that the scheme aims to protect against a non-targeted attacker that performs a physical observation (not video-, or camera-based) attack. Similarly to the APU concept, attackers are only able to perform an "online" attack, meaning that they have limited attempts to guess the passcode before the device gets locked.

3 Proposed Scheme

Our proposed scheme adopts design concepts from the APU and uses symbols as the building blocks of the password (Figure 1). We use the familiar 3x3 grid setting from Android and the method of forming the password by swiping the finger among different nodes on the grid. However –different from Android which uses a static grid– we propose the use of a dynamic grid that keeps changing



(a) Static (b) Dynamic (c) Numbering (d) Neighbors

Fig. 1. The Android pattern lock screen grid (**a**), and an instance of the ever-changing Bu-Dash grid (**b**). Part (**c**) shows the nomenclature for the nodes' positions and Part (**d**) demonstrates eligible moves to neighbor nodes from position β. Blue color indicates "knight moves" [5].

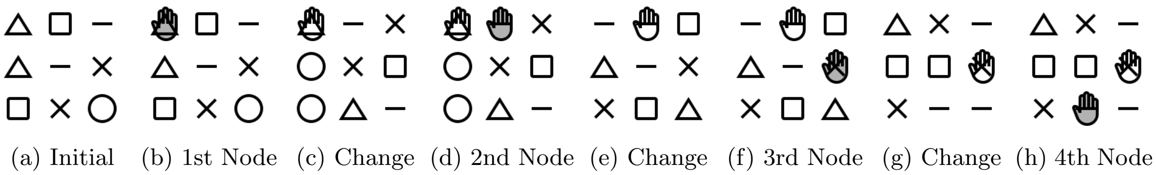
when the users swipe their fingers (Fig. 1b, 2). We believe that this addition to the password scheme will make the authentication process more resistant to shoulder surfing attacks. The `Bu-Dash` grid is not static and it does not feature only bullet points as nodes (like the Android's grid, see Fig. 1a). The `Bu-Dash` grid is dynamic and it includes 5 different shapes as nodes (Fig. 1b). The nodes (shapes) are randomly chosen and fetched by the system when the password scheme launches and they keep changing when users swipe their fingers to select the next node in the password chain. We implemented the following guidelines to assist users to get familiar with `Bu-Dash` passwords.

- The password is formed as a sequence of shapes from the following set of symbols: {○, □, −, △, ×}
- *Length*: The preferred password must be 4 – 9 shapes long.
- *Diversity*: The preferred password must contain at least 2 different shapes.
- Passwords are formed when users swipe their fingers on a 3x3 grid that keeps changing when they visit a new position.
- *Allowed moves*: Users are allowed to swipe their fingers in the neighbor nodes only, therefore "jumps" to a distant node are not feasible (e.g. from β to θ in Fig. 1c), unless they chose a "knight move" [5], (as seen in Fig. 1d).
- Users are allowed to revisit a node on the grid as many times they need.

Figure 2 shows an example of a user forming the following password to unlock a device: △−×−

4 Methodology

First, we conducted an online survey requesting respondents (Android and iOS users) to provide a `Bu-Dash` password that they would use on their devices. The request was to provide an *"easy-to-use and secure password"*. In this digital "pen-and-paper" study, participants were not interacting with a device. They were asked to envision a *usable* and *secure* `Bu-Dash` password based on the constrains mentioned in Section 3. They also had the chance to view a short video



(a) Initial (b) 1st Node (c) Change (d) 2nd Node (e) Change (f) 3rd Node (g) Change (h) 4th Node

Fig. 2. Example: Forming the password $\triangle - \times -$: The starting grid (a) shows the 5 shapes in random order. Users can place their fingers to any node featuring the $\triangle$ shape (b) and the node will become visited. At that moment, the shapes on the grid change randomly (c) and the user tries to reach the next shape of the password, which is – (d) swiping to position β. The – is reached and the grid changes again (e). The same process continues until the full password is formed (f - h). Notice the variety of options the user has to visit positions ζ or η in Fig. 2e, and positions γ, θ, or ι in Fig. 2g.

that was explaining how the scheme works and showing an example about how they can swipe their fingers on the dynamic grid to form a password. We did not show any examples about how to form a certain password aiming to avoid introducing unwanted biases. Our primary intention was to gather information about how intelligible the proposed scheme is. Additionally, we asked the participants if they would prefer this scheme over the traditional APU. In this paper we refer to this group of participants as the "**Survey**" group *(n = 65)*. The survey was communicated to a diverse mix of students and staff via emails and announcements in the learning platform of our Institution. We received responses from 85 individuals (who joined anonymously), but only 65 consented in participating and answered all given questions. As an incentive for their participation, individuals were included in a raffle to win vouchers.

At a second phase, we assessed users' interactions with the proposed scheme. We developed an application, titled "Bu-Dash", which was distributed via the Google Play app store in the "Education" category. The application was featuring the `Bu-Dash` password grid and captured initially participants' input. The application was later updated to acquire very basic usability features at the latter stages of our experiments. We released the first edition of the Bu-Dash application on Google Play and asked a small group *(n = 14)* of Android users (utilizing the same communication channels as previously) to interact with the `Bu-Dash` grid and provide passwords they would use on their devices. We refer to these respondents as the "**Pilot**" group in this work.

Participants were asked to download our application on their Android devices and then launch it. The application asked them to provide basic demographics (gender, age, education), and answer some generic, multiple-choice questions (mobile OS they use, if they were familiar with the APU, and which kind of authentication they use on their devices). Afterwards, participants viewed a set of instructions about how to create a `Bu-Dash` password. It should be noted that the sequence of shapes was randomized every time the user was looking at the instructions. We followed this strategy to assess if provided passwords were affected by the first shape the users were seeing in the instructions. Finally, respondents were asked to form their preferred Bu-Dash password on their devices. Mimicking the same process while forming an APU passcode, the application was asking the participants (as a final step) to re-enter and confirm their Bu-Dash password. Additionally, users had the choice to be included in a raffle to win vouchers and then exit the application.

The application was updated at a later stage as we were aiming to review usability characteristics of the proposed scheme. We added a "Memory Game" to the application and asked a different group of participants to play. Users had the choice to play any of the "Easy", "Medium", "Hard" levels. The rules of the game were simple. After viewing the formation of (let's say) an "Easy" password on the Bu-Dash grid (i.e., a sequence of 4 shapes: ×○×□), they were asked to re-enter this password. They were also given the chance to watch again the password formation on their screens as many times as they wanted. The "Medium" password consisted of 6 shapes and the "Hard" one consisted of 9 shapes. We did not use any complexity metrics [2] for this task, because our primary goal was to figure out if users would be able to recall at least a 4-node password. Therefore, we were aiming to assess the *short-term memorability* of the scheme. In this paper we refer to these participants as the auxiliary or "**Aux**" group *(n = 18)*.

5 Results

First, we present results derived from the "Survey" group, comprising individuals that did not have access to the Bu-Dash application via their devices. Then, we discuss outcomes derived from two different user groups (namely "Pilot" and "Aux") of our Bu-Dash application which utilized the proposed password scheme. Our aim is to identify common traits (if any) and attempt an initial assessment of Bu-Dash's usability features.

5.1 Password Space

Looking at the Bu-Dash password design constrains we recall that the passcode must be at least 4 shapes long and its length can be up to 9 nodes. There are 5 different available shapes to choose from and there must be at least 2 different shapes in the password. Neighbor nodes can be visited as many times as necessary to form the password and the system ensures that there always exists at least one available shape (from the set of the 5) in the neighborhood of a visited node. This means that there exist $5 \cdot 5 \cdot 5 \cdot 5 - 5 = 620$ different 4-node Bu-Dash passcodes. Similarly, there are $\underbrace{5 \cdot 5 \cdot 5 \ldots 5 \cdot 5}_{9\ nodes} - 5 \approx 1.9M$ different combinations to form a 9-node passcode. We exclude those combinations that contain the same symbols in each passcode, e.g., those similar to ○○○○ for a 4-node passcode. Thus, we have more than 2.4M unique passcodes under this scheme (i.e., 2,441,220). Therefore, Bu-Dash's password space is more than 6 times bigger than the one defined by the APU scheme (which has 389,112 unique passcodes [1, 28]). However, the APU has a wider space (if we consider that options are equiprobable) when we focus on passwords with 4-6 nodes.

5.2 "Survey" Group

Most participants in the treatment group were undergraduate students (72%). In the "Survey" group most respondents identified as males (66%), and iOS users (78%), but the majority (94%) was familiar with the APU. In this survey we were basically targeting respondents that did not have access to the Bu-Dash application; this explains the prevalence of iOS users in the sample. Most participants (94%) said they use a passcode on their devices and the majority (72%) prefer biometric authentication methods (Fingerprint/Face ID). After providing basic demographics, the participants saw a sequence of the available Bu-Dash shapes (○-△□×) and instructions about how to form a *valid* Bu-Dash password. We then asked them the following open-ended questions:

- **Q1**: "Write down the passcode you chose (C for circle, D for dash, T for triangle, S for square, X for X), e.g. CDCDCC".
- **Q2**: " Would you use the "Bu-Dash" passcode scheme on your device? Which scheme you would use: a) Android Pattern Lock, or b) Bu-Dash? Please explain why.

Below we discuss insights resulted from their responses.

The Bu-Dash scheme is comprehensive Although we did not offer any mechanisms to validate correct formation and input of the provided Bu-Dash passwords, invalid entries were not identified **(Q1)**. Thus, we deduce that the scheme is intelligible and the provided instructions are sufficient and comprehensive.

Password Characteristics We gathered statistics from the acquired passwords, and we discuss them here (see Table 1). We mentioned previously that participants saw a sequence of the shapes they should use to create their Bu-Dash passwords and we said that the circle was the first symbol in the sequence: (○-△□×). This might have created a bias towards starting their passwords with a ○, because 22 participants (i.e., approximately 1/3) created a password featuring a ○ as a starting point. In the next sections we discuss how we managed to overcome this issue by randomizing the shapes we show first in the tutorial part of the Bu-Dash application. Additionally, we noticed that the - and the × symbols were the least favorite to start a password in this sample of users. We also estimated how many times the distinct shapes appear in the set and we report that their frequency is almost uniform (with approximately 51 appearances each). Finally, □ and - appear to be used less frequently than the other symbols, with 46 and 44 appearances, respectively.

Table 1. Password Characteristics of "Survey" Password Set

Password Characteristics	○	□	−	△	×
N^o of passwords starting with shape:	**22**	14	8	12	9
N^o of times appeared in password set:	51	46	44	51	51

Table 2. Frequency Analysis of "Survey" Password Set

Password Length Frequency			**Shapes Used per Password**		
Length	Freq.	%	Shapes N^o	Freq.	%
4	12	18.46%	2	8	12.31%
5	10	15.39%	3	19	29.23%
6	**18**	**27.69%**	4	**21**	**32.31%**
7	12	18.46%	5	17	26.15%
8	5	7.69%	**Length**: $\mu = 6.185$, $\sigma = 1.580$		
9	8	12.31%	**Shapes**: $\mu = 3.723$, $\sigma = 0.992$		

We also gathered frequency analysis results (see Table 2). Most participants created a password with 6 nodes (18 respondents) and 21 respondents used 4 shapes in their passwords. One can deduce that the "Survey" participants were mostly focused on the proposal of a secure password because they did not have the opportunity to actually use the `Bu-Dash` scheme on their devices. Therefore, we report the following attributes of the provided password set. For the length of the passwords we have $\mu = 6.185$ and $\sigma = 1.580$ (μ: mean, σ: standard deviation). The median value of the password length is 6 and the median value of the number of shapes per password is 4.

Qualitative Study - Biometrics Prevalence Finally, we taxonomized respondents' answers to **Q2** in a qualitative codebook. Recall that the majority of respondents are iOS users (51 respondents) and they utilize biometric authentication on their devices. However, 23 people in the sample (of 65) expressed positive views regarding the use of a `Bu-Dash` password on their devices (e.g., **P51**: *"Yes, because you could easily remember the shapes"*). Additionally, 6 participants did not use a strong positive word (i.e., "Yes", "Definitely", etc.) and they were taxonomized as neutral. However, they eventually expressed a positive attitude towards the proposed scheme: e.g., **P42**: *"On a mobile device I would try it out. I like the idea that it moves about"*. Positively inclined respondents basically commented on the usability and security that `Bu-Dash` provides: **P61**: *"Yes, it provides improved security for my device and is easy"*, and: **P41**: *"Cause it the same concept as using numbers its secure and easy to remember"*.

Negative answers for using `Bu-Dash` were basically focused around users' convenience with current methods and biometric authentication (13 users). However, we should recall that knowledge-based methods are still important, because they are required as a complimentary method of authentication, in case the device remains idle for a long time (or after it restarts), or in case the biometric sensors fail (especially in the COVID era, when users wear face masks in closed spaces, thus methods such as “FaceID” are not –currently– usable). Although **Q2** requested from users to choose whether they would use a Bu-Dash or an APU password, several participants seem they would not give up the convenience provided by biometrics. This was made clear in their responses: e.g., **P49**: *“No, because Face ID is much faster”*. However, if we ignore these responses (given that they did not comment on their preference between the APU or Bu-Dash, but they just advocated for biometrics) we can see that the same amount of people in our sample are positively (29), or negatively (28) inclined to use Bu-Dash. *Note:* Considering that 6 participants expressed a neutral view but they were eventually more keen to adopt the proposed scheme: e.g., **P52**: *“Maybe, it seems like an interesting and puzzling way to make your phone secure”*.

5.3 “Pilot” Group

Similar to the “Survey” group, participants in the “Pilot” group of users were mostly undergraduate students (79%), identified as males (71%), using biometric authentication (57%) and their main device was running Android (79%). This group was the first to use the Bu-Dash scheme on their devices; therefore, insights from provided passwords are very useful to understand the usability and security of the scheme. We gathered their responses to compare them with our initial results derived from the “Survey” group.

Starting Point In Section 5.2 we discussed the possible bias our survey intructions might have introduced regarding the starting point of the provided passwords. The Bu-Dash’s application instructions however were illustrating the shapes in random order every time they were fetched, aiming to eliminate similar biases. Furthermore, we tracked the sequence of shapes shown in the instructions during our experiments and compared them with the provided passwords from the users. The results demonstrate that only 2 of the 14 users provided a password that started with the same shape as the one that was firstly depicted in the instructions. Therefore, we believe that our updated tutorial instructions do not subconsciously introduce biases. Additionally, Table 3 shows that the majority of the “Pilot” participants preferred to start their password with a ×. Furthermore, the × is the most common symbol that appeared in this password set.

Using the Bu-Dash Grid A comparison between Table 4 with the results reported in Section 5.2 shows that although users envision and formulate on paper long and complex passwords (length: $\mu = 6.185$; shapes included: $\mu = 3.723$) aiming to advance security, they eventually end up with shorter and less complex passwords (length: $\mu = 5.214$; shapes included: $\mu = 2.786$) the first time they formulate a Bu-Dash “phrase” on their devices (median length: 5; median N^o of shapes 2.5). This is a common trend in grid-based password authentication [2].

Table 3. Password Characteristics of "Pilot" Password Set

Password Characteristics	○	□	−	△	×
N^o of passwords starting with shape:	3	2	1	0	**8**
N^o of times appeared in password set:	8	7	5	6	**13**

Table 4. Frequency Analysis of "Pilot" Password Set

Password Length Frequency			**Shapes Used per Password**		
Length	Freq.	%	Shapes N^o	Freq.	%
4	6	**42.86%**	2	7	**50.00%**
5	3	21.43%	3	3	21.43%
6	3	21.43%	4	4	28.57%
7	0	0%	5	0	0%
8	2	14.28%	**Length**: $\mu = 5.214$, $\sigma = 1.424$		
9	0	0%	**Shapes**: $\mu = 2.786$, $\sigma = 0.893$		

Thus, in this treatment we can see that most respondents created a password with 4 nodes and half of the participants used 2 different shapes only. However, we advocate that the dynamic grid and the randomized order of the `Bu-Dash` starting grid are adequate to minimize shoulder surfing and smudge attacks. Additionally, although the majority of participants in this group provided shorter passwords, we believe that the proposed scheme is more secure compared to the APU. Recent research illustrated [1] that due to common biases when users form APU passcodes (e.g. starting from top left), its available password space decreases dramatically (more than 90% for 4-node passcodes). Additionally, it is more feasible to extract parts of an APU password via observation (and then perform a guessing attack) because an attacker can easily recall edges that link nodes, making the whole password less secure. On the contrary, `Bu-Dash` nodes are not visually linked with edges, thus an attacker cannot easily infer the next node in the password if a node is known.

To conclude, Tables 3 and 4 showcase that the most favorite shape to begin a `Bu-Dash` passcode in this treatment was the ×. This shape also appears often in the password set along with ○. The least used symbol in the "Pilot" password set is the -. Additionally, as stated in the previous paragraphs, users in this treatment valued usability more than security and preferred less busy passcodes compared to the "Survey" participants.

5.4 "Aux" Group

The "Aux" treatment contained mainly participants identified as males (78%), Android users (83%), familiar with the APU (89%), using biometric authentication on their devices (67%). 56% were undergraduate students and the rest had at least one University degree. Results derived from this group's provided data (Tables 5 and 6) confirm that when respondents use the `Bu-Dash` grid,

Table 5. Password Characteristics of “Aux” Password Set

Password Characteristics	○	□	−	△	×
N^o of passwords starting with shape:	3	2	0	5	**8**
N^o of times appeared in password set:	**14**	6	5	12	13

Table 6. Frequency Analysis of “Aux” Password Set

Password Length Frequency			**Shapes Used per Password**		
Length	Freq.	%	Shapes N^o	Freq.	%
4	10	**55.6%**	2	6	33.33%
5	5	27.78%	3	10	**55.56%**
6	1	5.55%	4	2	11.11%
7	0	0%	5	0	0%
8	2	11.11%	**Length**: $\mu = 4.833$, $\sigma = 1.295$		
9	0	0%	**Shapes**: $\mu = 2.778$, $\sigma = 0.647$		

they seem they choose shorter and less complex passcodes (length: $\mu = 4.833$; shapes included: $\mu = 2.778$). Median values for length is 4 and for the number of included shapes is 3.

Frequency Analysis Tables 5 and 6 confirm trends we saw in the “Pilot” treatment. × is the most preferred starting shape in this treatment too (44.4%). Since this is not a large scale study (we report preliminary results here) we can only note that this finding might introduce security concerns related to the available password space, similarly with the APU scheme as commented in Section 5.3. However, provided data from participants that interacted with the `Bu-Dash` grid (both from “Pilot” and “Aux” treatments) show that 68.75% of users that formed a short `Bu-Dash` code (4-nodes), preferred to include at least 3 shapes in their passcode. Therefore, we can see from these data that users value security when forming easy-to-use passcodes aiming to add more shapes in the sequence. Additionally, similar to Section 5.3, “Aux” data show that the − is the least used shape in the password set.

Commonly Used Passwords Another noteworthy finding is that we did not encounter any particular passcode to be prevalent in the whole password set (Survey-Pilot-Aux, namely *S.P.A.*). We recognize that reported results come from a limited sample of participants ($n = 97$) and that diversity in the provided passcodes should be expected. However, only 5 different passcodes were seen to exist –twice– in the provided data. These are as follows: △○××, ×○×□, ○□△×○, ×××□□□, ×△×△×△×△.

Preliminary Usability Assessment We asked the “Aux” Group’s respondents to participate in a Memory Game that was added in the final iteration of

Table 7. Memory Game Completions

Level	**Attempted**	**Completed**	**Average attempts to completion**	**Failed/no completion**	**Failure Rate**
Easy	18	17	1.13	1	5.6%
Medium	12	8	1.88	4	33.3%
Hard	5	3	2.67	2	40.0%

our experiments. As explained in Section 4, respondents were asked to play a Memory Game which featured 3 complexity levels ("easy", "medium", "hard"). We did not explicitly tell them how many levels they should attempt to play. As we did not use any complexity metrics to assess how difficult it would be for an individual to memorize these passcodes, we randomly formulated one 4-node, one 6-node, and one 9-node passcode as an "easy", "medium", and "hard" `Bu-Dash` password, respectively. Participants would choose the level of complexity they would like to play, and then they would see the password while it was formed on their screens. There was no limit on how many times they would watch the tutorial. Afterwards, they had to recall and form that password on the `Bu-Dash` grid. The Bu-Dash application logged how many times they tried to play a game and if they successfully recalled the passcode. Results are as follows (see Table 7).

Most participants in the "Aux" Group attempted to play the *Easy* game, but only 8 and 5 tried to solve the *Medium* and *Hard* levels, respectively. Seventeen users watched and successfully completed the *Easy* challenge; the average number of attempts to completion was approximately 1.13 attempts. Two participants of this group were considered as outliers and were excluded from the former estimation as they seemed they did not manage to complete the challenge after a reasonable number of attempts (more than 10 attempts each). The *Medium* challenge was undertaken by 12 individuals, and 8 of them successfully completed it with an average of 1.88 attempts. The *Hard* challenge was attempted by only 5 respondents; 3 of them successfully formed the –admittedly– challenging to recall password with an average of 2.67 attempts. These numbers confirm the expectation that when a password becomes longer, it eventually gets less usable and difficult to recall. However, there exist passcodes like the following one that are long, but very memorable: ×××□□□○○○. Thus, password length is not the only feature that contributes to complexity. Further experiments are needed to properly assess long-term memorabiltiy and the effects of password length in the password's complexity.

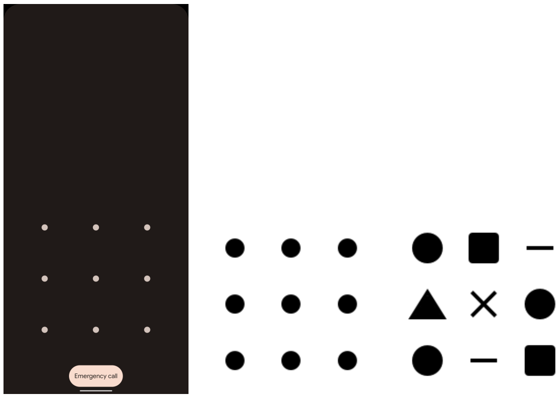
6 Discussion

We envisioned an authentication system that would be easy to comprehend and adopt, and at the same time, it would be secure against smudge attacks and shoulder surfing. We believe that `Bu-Dash` is a universal scheme because it can be employed for user authentication in various settings. It can be utilized on smartphones and tablets, or it can be adjusted to work on even smaller screens (e.g., smartwatches). Our proposed method can be fit for use on portable computers (using a trackpad, or the mouse) and desktops. It is also *universal* because its building blocks are common shapes that can be recognized and used easily by any human. Therefore, there are no language, or other cultural, or education burdens that could discourage people from using it.

Its dynamic 3x3 interface ensures that users will not feel unfamiliar with the authentication process. Bu-Dash works similarly with the APU, requiring users to swipe their fingers on the mobile device screen in order to form the password. Compared to the APU, it has less restrictions (for example, a node can be visited as many times as needed) and its password space is 5 times larger. Our online survey indicated that the scheme is comprehensive and easy to perceive because respondents ("Survey" Group), did not provide any invalid passwords when asked to create one after reading our basic instructions.

By looking at the passwords provided by participants from groups "Pilot" and "Aux" (they actually interacted with Bu-Dash on their devices providing valuable, real world data) we can infer that the scheme provides the opportunity to diversify users' input compared to the APU. We did not find several repeating passcodes, but we recognize that our sample is not extended enough. However, we only saw a few trends in the sample that might be linked with human habits; e.g., the preference in using × as a starting point, or the fact that - seems to be the least favorite shape to use in general. Additionally, our analysis demonstrated that when participants were asked to form a Bu-Dash passcode on their devices, they chose *shorter* passcodes aiming probably to make them more memorable and usable. However, early indications show that while they were choosing short passcodes, they also aimed to *add complexity* to the passcode using at least three shapes.

In this paper we report preliminary usability results. Although our data are credible (because they come from users that interacted with our scheme on their actual devices), we cannot confirm if they generalize well. This is a limitation of this paper. The collected Bu-Dash passcodes, derived by 97 participants in different settings, along with their associated metadata might provide a good first impression of how users would utilize the scheme, but there needs to be a longitudinal and large-scale study that would confirm the results provided in this paper. The collection of a larger dataset in the future will enable us also to perform a more robust security analysis using metrics, such as *α-guesswork ($\tilde{G_\alpha}$)* or *β-success rate*, as proposed by Bonneau [7]. In this work we talked about the password space defined by the Bu-Dash scheme and we mentioned that it is larger from the one defined by the APU. However, the set of unique Bu-Dash passcodes with a shorter length is smaller than the one in the APU scheme. As discussed in Section 5, Android pattern formation is usually driven by human habits and biases, significantly shortening the password space. We advocate that Bu-Dash is a secure authentication method because it uses a dynamic grid which is randomly initialized every time it is launched.



(a) APU (b) APU Grid (c) Bu-Dash Adjustment

Fig. 3. Potential Adjestments in the Use of the `Bu-Dash` Scheme.

Furthermore, in Fig. 3 we propose an adjustment for the `Bu-Dash` scheme that adhere to the APU design concepts. Fig. 3b shows the current static APU grid embedded in any Android version. Our analysis and results are based on data derived from volunteers that engaged with the `Bu-Dash` grid as shown in Fig. 2. However, Fig. 3c features a more precise adaptation of the `Bu-Dash` scheme to the APU design concept. It would be useful as future work to see if there exist any significant implications if the latter design prevails as a preferred visual improvement. Additionally, it would be interesting to see how additional variations of our proof of concept would affect usability and security (e.g., utilizing more than 5 symbols as building blocks, although this change might require further adjustments to the design constrains).

Ethical Considerations Volunteers provided informed consent before participating in the study. No identifiable data were stored and we cannot foresee any ethical issues deriving from our research, as it relates and presents a proof of concept which is not employed yet as a real authentication system on the participants' mobile devices. All volunteers were encouraged to uninstall our Bu-Dash application when they concluded their participation.

7 Conclusion

We presented a novel graphical password scheme, named `Bu-Dash`. `Bu-Dash`'s users create passcodes comprising sequences of simple shapes in an intuitive manner. We conducted a series of studies asking volunteers to interact with `Bu-Dash` and gathered data that allow us to report a positive attitude towards adopting the scheme as a primary authentication method for mobile devices. Preliminary results demonstrate the scheme's diversity and its extended password space. The dynamic grid features randomly mapped edges that constitute the basis of the Bu-Dash scheme and ensures that the authentication process is secure against smudge attacks and shoulder surfing. However, we noticed some human biases against using specific shapes (e.g., -) and we concluded that the users in our sample mostly preferred to start their passcodes with a certain symbol (×). Finally, we assessed basic usability features and reported that the scheme seems to be comprehensive, and usable. To conclude, this paper demonstrated the feasibility of adopting the proposed scheme as a user authentication method that can be employed in multiple settings, ranging from smartphones to desktops, and other (portable) devices.

Acknowledgments

Dr Panagiotis Andriotis was an International Research Fellow of Japan Society for the Promotion of Science (Postdoctoral Fellowships for Research in Japan (Standard)) when this paper was published.

References

1. Andriotis, P., Oikonomou, G., Mylonas, A., Tryfonas, T.: A study on usability and security features of the Android pattern lock screen. Information and Computer Security **24**(1), 53–72 (2016). https://doi.org/10.1108/ICS-01-2015-0001
2. Andriotis, P., Tryfonas, T., Oikonomou, G.: Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In: Tryfonas, T., Askoxylakis, I. (eds.) Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2014), Held as Part of HCI International 2014, Crete, Greece, June 22-27, 2014. pp. 115–126. Springer International Publishing (2014). https://doi.org/10.1007/978-3-319-07620-1_11
3. Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C.: A Pilot Study on the Security of Pattern Screen-lock Methods and Soft Side Channel Attacks. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. pp. 1–6. WiSec '13, ACM, New York, NY, USA (2013). https://doi.org/10.1145/2462096.2462098
4. Aviv, A.J., Budzitowski, D., Kuber, R.: Is bigger better? comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In: Proceedings of the 31st Annual Computer Security Applications Conference. p. 301–310. ACSAC 2015, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2818000.2818014, https://doi.org/10.1145/2818000.2818014
5. Aviv, A.J., Davin, J.T., Wolf, F., Kuber, R.: Towards baselines for shoulder surfing on mobile authentication. In: Proceedings of the 33rd Annual Computer Security Applications Conference. p. 486–498. ACSAC 2017, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3134600.3134609, https://doi.org/10.1145/3134600.3134609
6. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX Conference on Offensive Technologies. p. 1–7. WOOT'10, USENIX Association, USA (2010)

7. Bonneau, J.: The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In: 2012 IEEE Symposium on Security and Privacy. pp. 538–552 (2012). https://doi.org/10.1109/SP.2012.49
8. Chen, Y.L., Ku, W.C., Yeh, Y.C., Liao, D.M.: A simple text-based shoulder surfing resistant graphical password scheme. In: 2013 International Symposium on Next-Generation Electronics. pp. 161–164 (2013). https://doi.org/10.1109/ISNE.2013.6512317
9. Cho, G., Huh, J.H., Cho, J., Oh, S., Song, Y., Kim, H.: Syspal: System-guided pattern locks for android. In: 2017 IEEE Symposium on Security and Privacy (SP). pp. 338–356 (2017). https://doi.org/10.1109/SP.2017.61
10. Dai, L., Zhang, K., Zheng, X.S., Martin, R.R., Li, Y., Yu, J.: Visual complexity of shapes: a hierarchical perceptual learning model. The Visual Computer pp. 1–14 (2021)
11. De Angeli, A., Coventry, L., Johnson, G., Renaud, K.: Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies **63**(1), 128–152 (2005). https://doi.org/https://doi.org/10.1016/j.ijhcs.2005.04.020, https://www.sciencedirect.com/science/article/pii/S1071581905000704, hCI research in privacy and security
12. De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M.E., Slawik, B.E., Hussmann, H., Smith, M.: Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. p. 2937–2946. CHI '14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2556288.2557097, https://doi.org/10.1145/2556288.2557097
13. Forman, T., Aviv, A.: Double patterns: A usable solution to increase the security of android unlock patterns. p. 219–233. ACSAC '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3427228.3427252, https://doi.org/10.1145/3427228.3427252
14. Gugenheimer, J., De Luca, A., Hess, H., Karg, S., Wolf, D., Rukzio, E.: Colorsnakes: Using colored decoys to secure authentication in sensitive contexts. In: Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services. p. 274–283. MobileHCI '15, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2785830.2785834, https://doi.org/10.1145/2785830.2785834
15. Kabir, M.M., Hasan, N., Tahmid, M.K.H., Ovi, T.A., Rozario, V.S.: Enhancing smartphone lock security using vibration enabled randomly positioned numbers. In: Proceedings of the International Conference on Computing Advancements. ICCA 2020, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3377049.3377099, https://doi.org/10.1145/3377049.3377099
16. Khan, H., Hengartner, U., Vogel, D.: Evaluating Attack and Defense Strategies for Smartphone PIN Shoulder Surfing, p. 1–10. Association for Computing Machinery, New York, NY, USA (2018), https://doi.org/10.1145/3173574.3173738
17. Kim, S.H., Kim, J.W., Kim, S.Y., Cho, H.G.: A new shoulder-surfing resistant password for mobile environments. In: Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication. ICUIMC '11, Association for Computing Machinery,

New York, NY, USA (2011). https://doi.org/10.1145/1968613.1968647, https://doi.org/10.1145/1968613.1968647

18. Ku, W.C., Liao, D.M., Chang, C.J., Qiu, P.J.: An enhanced capture attacks resistant text-based graphical password scheme. In: 2014 IEEE/CIC International Conference on Communications in China (ICCC). pp. 204–208 (2014). https://doi.org/10.1109/ICCChina.2014.7008272
19. Kwon, T., Na, S.: Switchpin: Securing smartphone pin entry with switchable keypads. In: 2014 IEEE International Conference on Consumer Electronics (ICCE). pp. 23–24 (2014). https://doi.org/10.1109/ICCE.2014.6775892
20. Kwon, T., Na, S.: Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. Computers & Security **42**, 137–150 (2014). https://doi.org/https://doi.org/10.1016/j.cose.2013.12.001, https://www.sciencedirect.com/science/article/pii/S0167404813001697
21. Kwon, T., Na, S.: Steganopin: Two-faced human–machine interface for practical enforcement of pin entry security. IEEE Transactions on Human-Machine Systems **46**(1), 143–150 (2016). https://doi.org/10.1109/THMS.2015.2454498
22. Lee, M.K.: Security notions and advanced method for human shoulder-surfing resistant pin-entry. IEEE Transactions on Information Forensics and Security **9**(4), 695–708 (2014). https://doi.org/10.1109/TIFS.2014.2307671
23. Loge, M., Duermuth, M., Rostad, L.: On user choice for android unlock patterns. In: European Workshop on Usable Security, ser. EuroUSEC. vol. 16 (2016)
24. Markert, P., Bailey, D.V., Golla, M., Dürmuth, M., Aviv, A.J.: This pin can be easily guessed: Analyzing the security of smartphone unlock pins. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 286–303 (2020). https://doi.org/10.1109/SP40000.2020.00100
25. Munyendo, C.W., Grant, M., Philipp Markert, P., Forman, T.J., Aviv, A.J.: Using a blocklist to improve the security of user selection of android patterns. In: Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021). USENIX Association (Aug 2021), https://www.usenix.org/conference/soups2021/presentation/munyendo
26. Schneegass, S., Steimle, F., Bulling, A., Alt, F., Schmidt, A.: Smudgesafe: Geometric image transformations for smudge-resistant user authentication. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. p. 775–786. UbiComp '14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2632048.2636090, https://doi.org/10.1145/2632048.2636090
27. Song, Y., Cho, G., Oh, S., Kim, H., Huh, J.H.: On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks, p. 2343–2352. Association for Computing Machinery, New York, NY, USA (2015), https://doi.org/10.1145/2702123.2702365
28. Sun, C., Wang, Y., Zheng, J.: Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications **19**(4), 308–320 (2014). https://doi.org/https://doi.org/10.1016/j.jisa.2014.10.009, https://www.sciencedirect.com/science/article/pii/S2214212614001458
29. Tupsamudre, H., Banahatti, V., Lodha, S., Vyas, K.: Pass-o: A proposal to improve the security of pattern unlock scheme. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. p. 400–407. ASIA CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3052973.3053041, https://doi.org/10.1145/3052973.3053041

30. Uellenbeck, S., Dürmuth, M., Wolf, C., Holz, T.: Quantifying the security of graphical passwords: The case of android unlock patterns. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. p. 161–172. CCS '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2508859.2516700, https://doi.org/10.1145/2508859.2516700
31. Vaddepalli, S., Nivas, S., Chettoor Jayakrishnan, G., Sirigireddy, G., Banahatti, V., Lodha, S.: Passo – new circular patter lock scheme evaluation. In: 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services. MobileHCI '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3406324.3417167, https://doi.org/10.1145/3406324.3417167
32. Wang, D., Gu, Q., Huang, X., Wang, P.: Understanding human-chosen pins: Characteristics, distribution and security. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. p. 372–385. ASIA CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3052973.3053031, https://doi.org/10.1145/3052973.3053031
33. Ye, G., Tang, Z., Fang, D., Chen, X., Wolff, W., Aviv, A.J., Wang, Z.: A video-based attack for android pattern lock. ACM Trans. Priv. Secur. **21**(4) (Jul 2018). https://doi.org/10.1145/3230740, https://doi.org/10.1145/3230740
34. von Zezschwitz, E., De Luca, A., Brunkow, B., Hussmann, H.: SwiPIN: Fast and Secure PIN-Entry on Smartphones, p. 1403–1406. Association for Computing Machinery, New York, NY, USA (2015), https://doi.org/10.1145/2702123.2702212
35. von Zezschwitz, E., Eiband, M., Buschek, D., Oberhuber, S., De Luca, A., Alt, F., Hussmann, H.: On quantifying the effective password space of grid-based unlock gestures. In: Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia. p. 201–212. MUM '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/3012709.3012729, https://doi.org/10.1145/3012709.3012729
36. Zimmermann, V., Gerber, N.: The password is dead, long live the password – a laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies **133**, 26–44 (2020). https://doi.org/https://doi.org/10.1016/j.ijhcs.2019.08.006, https://www.sciencedirect.com/science/article/pii/S1071581919301119