The Pattern-richness of Graphical Passwords

Johannes S. Vorster
Rhodes University
email: JSVorster@gmail.com
Barclays Africa
email: Jo.Vorster@absa.co.za

Renier P. van Heerden
Council for Scientific
and Industrial Research
email: renier@sanren.ac.za
Nelson Mandela Metropolitan University

Barry Irwin
Rhodes University
email: B.Irwin@ru.ac.za

***Abstract*—Conventional (text-based) passwords have shown patterns such as variations on the username, or known passwords such as ”password”, ”admin” or ”12345”. Patterns may similarly be detected in the use of Graphical passwords (GPs). The most significant such pattern – reported by many researchers – is hotspot clustering.**

This paper qualitatively analyses more than 200 graphical passwords for patterns other than the classically reported hotspots. The qualitative analysis finds that a significant percentage of passwords fall into a small set of patterns; patterns that can be used to form attack models against GPs. In counter action, these patterns can also be used to educate users so that future password selection is more secure.

It is the hope that the outcome from this research will lead to improved behaviour and an enhancement in graphical password security.

***Index Terms*—Information security, graphical passwords, password patterns, user authentication, user study.**

I. Introduction

A. Background

Historical and current research into Graphical Passwords (GPs) cover a rich topic; see [1] for a review, we present only a small overview. GPs were first explored as an alternative to text-based passwords in the early 1990s. The first patent on the topic was registered to G. Blonder in 1995 [2], based on the idea of sequentially selecting points on an image – see Figure 1 (a). In this schema the user enrols by selecting a number of points on an image. Authentication is then done by re-selecting the same points in the same order. Obviously the user cannot select the same point down to a pixel level, so the schema must inherently have some error margin. The size of the error region effectively defines a theoretical limit on the number of different passwords per image.

The initial idea from Blonder was soon followed by a variety of schemes that avoided the initial patent by using other mechanisms of schemes. Draw-a-Secret (DAS), abstractly proposed by Syukri et.al. [3] and later implemented by Jermyn et.al. [4], uses a blank grid canvas and records a password as a sequence of strokes. In this scheme, each stroke travels through a number of grid-elements, and these are recorded to form the password – see Figure 1 (b).

In the early 2000s a number of alternative schemes were proposed and implemented. PassFaces, proposed by Brostoff and Sasse [5], used facial images – see Figure 1 (d). In this scheme, the user enrols by selecting a number of faces from a large database of faces. During authentication one of the enrolment images are shown together with 8 other faces in a 3x3 grid. The user must go through a number of rounds, selecting the correct face from the 9 options during each round. Déjà Vu is a similar scheme proposed by Dhamija and Perrig [6]. It uses abstract – see Figure 1 (c). However it was shown during their study that enrolment rates for abstract images took twice as long as for face-based images.

Wiedenbeck et.al. [7] proposed a scheme called PassPoints that is similar to that of Blonder, but it makes use of photos and well-defined tolerance circles. As was pointed out, this scheme needs to define an effective area around the enrolment points to ensure successful authentication. In a study by Van Oosterchot & Thorpe [8], the effective grid must be 19x19 around the point of enrolment to minimize login failures but maximize key-space.

Tao [9] proposed a recall-based scheme based on the board game Go. Users connect points placed on the intersections of grid-lines. This schema is perhaps the grandfather of the Android pattern unlock mechanism used on smartphones.

Background DAS (BDAS) [10] puts a background image on the DAS grid, allowing users to have a cued recollection of their password. Jansen's Picture Password scheme [11] is perhaps the most usable cue-recall based

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

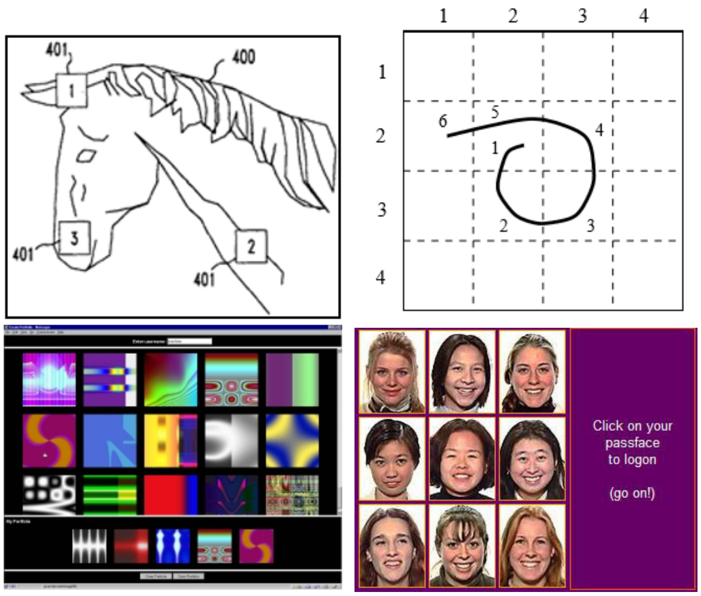

Fig. 1. Different graphical password schemes: (a: top-left) Blonder's original patent image; (b: top-right) Draw-a-secret example; (c: bottom-left) Deja-vu; (d: bottom-right) Pass-faces.

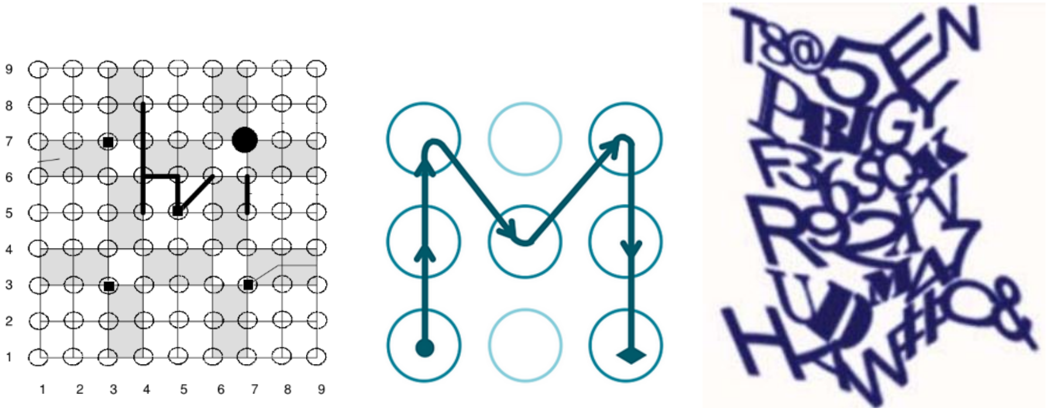

Fig. 2. Graphical password schemes: (a: left) Pass-Go; (b: middle) Android pattern unlock; (c: right) Captcha-based GP.

scheme; using a grid overlay on an image and numbering the grid elements rather than using the actual image coordinates. This schema is similar to BDAS, but instead of drawing an image on top of the background, the user selects points on the image similar to the original Blonder scheme.

GP schemes have been implemented on mobile devices, but due to physical constraints entering such passwords is error-prone, less secure and less effective than with physical keyboards [12]. Popular GP schemes used on smartphones – see Figure 2 (b) is nothing more than a replacement of a numeric password scheme. It has been shown that the Android pattern unlock is equivalent to a 5 digit numeric password [13]. In a 2015 study of the Android pattern unlock it was found that most passwords consist of two or three strokes and that there are directional biases (more left-to-right), but that the introduction of an over-lay image can improve this bias [14]. Another study found that 38% of passwords start in the top-left corner and that the combined percentage for starting in the bottom- center, bottom-right or right-middle, is only 8% [15].

More recently, alternatives have been proposed using more dynamic generation of images based on text-based passwords, such as the Captcha-based schema proposed by Gao, Wang and Dai [16]. The aim of such a GP scheme is to use hard Artificial Intelligence (AI) problems as a security primitive [17]. One obvious problem with such schemas is that it is strongly dependent on current technology and the entire scheme can be invalidated by new technology.

Other authors have proposed using GPs not for direct authentication but for secondary security processes, such as password recovery. For example, Almuairfi et.al. [18] proposes the use of GPs as a substitute to the security questions used during recovery of lost passwords.

Many conventional password proposals have been mapped to GP equivalents. An interesting such case is that of ”honeywords”; false passwords that are hashed and transmitted as part of normal password authentication. If such a password is used in an attempt to authenticate there is a high probability that the user's account has been compromised [19]. A similar scheme for GPs has been proposed [20].

B. Graphical Password Categories and Security

GPs can be categorized based on the mechanism that the users use to recall the correct password. There are three categories: recall-based, recognition-based and cue-based.

Recall-based schemes rely on the user remembering the password without any assisting framework. From the examples in the previous sections, DAS, Pass-Go and the Android pattern unlock are examples that fit into this category. These schemas have been extensively studied for security vulnerabilities.

Recognition-based passwords rely on the user recognizing an image from the password set from a larger set of images. Typical schemes in this group are PassFaces and Déjà Vu. One of the problems with such schemes are the number of rounds needed to enter passwords [10].

Cue-based passwords present the user with a cue, such as a background image on which a password is selected by clicking on the image. Blonder's original patent, Passpoints, BDAS and Jenson's scheme fall into this category. One of the most significant considerations when using such a scheme is that of hotspots, discussed below.

To use conventional passwords as a benchmark, studies [21] have found that conventional passwords have lengths between 6 and 13 characters with an average bit strength of 37.8 bits. Graphical passwords – for some schemes – have proven to give slightly stronger security [22]. PassPoints [7], for example, shows a significantly higher key-space size compared to conventional passwords. Using a background image for DAS – called BDAS – improves user password length [10].

One of the prominent critiques of GPs has been the threat of shoulder-surfing – an attacker observing the user during password entry. A significant number of proposals have been generated to counter this threat [23], [24], [25], [26], [27].

C. Graphical Password Patterns

In the Biddle et.al. review of graphical passwords, it is noted that the size of the graphical password key space may be significantly smaller than the theoretical calculations due to password patterns, as is the case with conventional passwords. User-biases during password selection has been reported in numerous studies [28], [10], [29], [30], [31].

One of the first patterns that was recognized as part of graphical password selection is hotspots. In cued-recall schemes the background image plays an important role in the strength of the password; images with a low number of features tend to create password hotspots, that is, a large subset of the user population selects the same points on the image as part of their password [31]. This can be seen as the analogue of conventional passwords that often are selected from a small subset of characters. For example, in the RockYou dataset of 32 million passwords, 20.5% of passwords are number-only passwords [32].

Dirik et.al. [33] constructed an image processing algorithm that uses heuristics to attempt to identify potential hotspots in images that are then used to guess PassPoints passwords. Using the heuristics, they generate a dictionary of size 2^{32} entries and test against the PassPoints password set with a theoretical 40-bit size and report an 8% success rate in cracking the user passwords. This is a low success rate and one explanation proposed is that the the implemented heuristics did not match the patterns that humans would pick [34].

Van Oorschot & Thorpe [8] used heuristics to crack passwords from a database of click-based passwords. They identified four patterns, and found that 56% of passwords contain patterns from their 4-set of patterns. The patterns are: horizontal (15%), vertical (15%), diagonal (11%) and clock (5%); where clock is a clockwise pattern – circular clockwise or circular anti-clockwise.

II. Methodology and Study Execution

A. Overview and Aim

In this study, we wanted to understand what the types of patterns are that humans use when selecting GPs. The earlier studies did not involve the participants directly, that is, they never asked the participants for the method used. Therefore, we opted to use a qualitative study rather than a quantitative approach.

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

The aims of this study are: identify the types of patterns that users employ for selecting GPs. How do these patterns change if users are made aware of obvious security considerations for GPs, such as hotspots.

The first section of the study involved the selection of images and schemes to use. Since significant studies have already been conducted on DAS passwords, we focus on click-based passwords through various image-selection schemes and employ a Jankens's type model [11].

The images used are presented in Figure 3. The Kitten and Hedgehog image, used by [35], [34], [36], was selected because of its low feature set. It is expected that these images should have a high hotspot incidence. The question we are interested in for these images are how the pattern changes after users are made aware of the hotspots they have selected as passwords. The Paperclip image was used by [8] and has a high number of features that should lead to few hotspots. The Company Logo image was generated using Interbrand and consists of some well-known brand icons. Such an image is similar to those used as alternatives to PassFaces and Déjà Vu. A critique often mentioned against PassFaces is that the passwords selected have patterns, such a all beautiful people or all women. The Faces image was included to investigate the password patterns in such images and to question users on why they had selected the passwords in these images.

B. Methodology

Interviews where held with 21 participants. During the interviews the five images were presented to the participants and they were asked to select passwords. Participants were also asked what the reason was for their password selection for each image. Once that was completed the participants were informed that graphical passwords are known for having hotspots or other patterns. Users were not shown any examples but told that in an image such as Kitten most users would select predictable points such as ears, eyes, nose and paws. No other images were referred to, nor were any other patterns pointed out, other than to mention that there are other patterns.

Participants were then asked if they wanted to revise their password selection and again had the opportunity to select passwords for the five images. Again participants were given the opportunity to identify the method that was used for the selection of the passwords.

The password patterns were analysed manually and classified. Password patterns were analysed and identified and also correlated with the reasons participants gave for their password patterns.

The participants were selected at random from a group of professionals that included project managers, business analysts, software developers and administrative staff.

III. Results and Discussion

Analysis of the passwords during the first enrolment support previous results that report a significant number of passwords that use hotspots. We find 22% of initial enrolment passwords conform to hotspot clusters – see Fig. 4 for the Kitten hotspots. If compared to the patterns reported by [8] we find the same patterns, but with smaller percentages. For example we find only 2% of patterns conform to a vertical lines pattern, and 3% to a diagonal lines pattern – see Table I. Some of the non-hotspot patterns that show up in the first enrolment data set are shown in Figure 5.

Through inspection and the participant interviews we identify patterns that are independent of the image itself; that is, we find patterns such as zig-zag, or border-based patterns.

To further extend the analysis we set up a new classification scheme. First we define a category called Lines, which consists of all three of the line categories from [8]; vertical, horizontal and diagonal lines. We find that 27/105, or 26%, of the passwords fall into the Lines category. We then define a Border pattern, consisting of all squares or graphical password points that are on the border of the image. From the data we find that 6/105 passwords follow this pattern. When we define a Zig-zag category as a one row or column zig-zag pattern, then only 2% of first enrolment passwords conform to this pattern.

For the Paperclip image we can define only one pattern, and that is a Colour pattern. We define a password as conforming to the Colour pattern if all the points are selected to be paper clips with the same colour. Our initial expectation was that Paperclip would be the most secure, since it has such a high number of features

TABLE I
Comparitive Patterns: First enrolment compared with Van Oorschot & Thorpe [8] Patterns

Pattern	Instances and percentage	Comparitive from [8]
Hotspots	24/105 = 22%	n/a
Vertical lines	2/105 = 2%	15%
Horizontal lines	8/105 = 8	15%
Diagonal lines	3/105 = 3%	11%
Clock	0/105 = 0%	5%

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

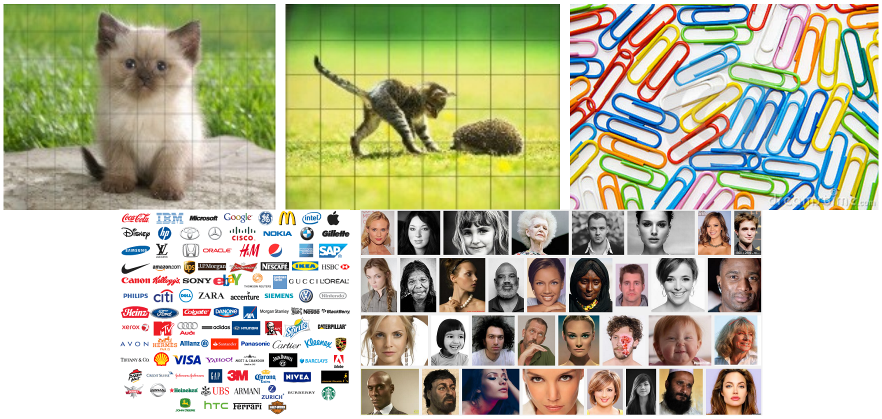

Fig. 3. Images used in the study: (a: top-left) kitten; (b: top-middle) hedgehog; (c: top-right) paperclip; (d: bottom-left) logos; (e: bottom-right) faces.

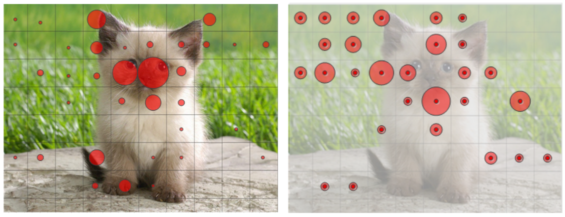

Fig. 4. Hotspot patterns between first (left) and second (right) enrolment.

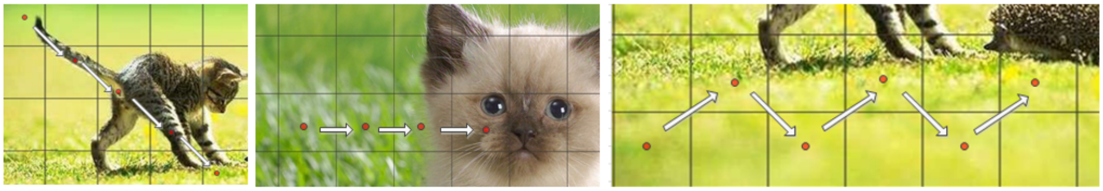

Fig. 5. Non-hotspot patterns found during 1st enrolment.

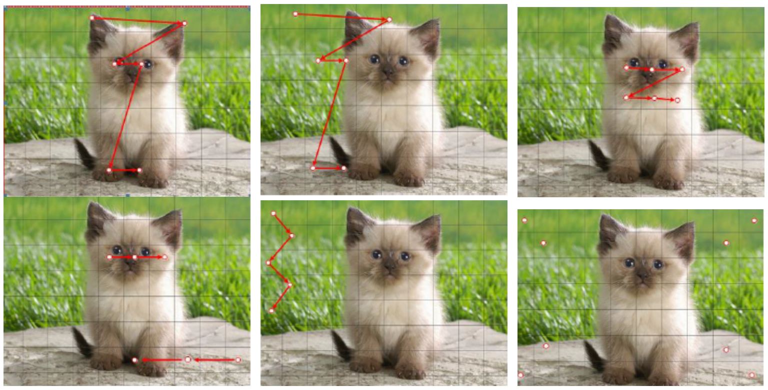

Fig. 6. Example-patterns found during enrolments. (top-left):hotspots; (top-middle):shifted hotspot; (top-right):independent, with hotspot offset; (bottom-left):combination dependent and independent; (bottom-middle):independent of picture; (bottom-right):corner-based pattern.

for the participants to select from. However, it turns out that 48% of passwords consists of a single or two-colour selection for the first enrolment. If the second enrolment's data is also included, then overall we find 33% of passwords conform to a one- or two colour pattern.

Lastly some passwords are clustered on a small number of points that located close to each other. If a 3x3 pattern is defined as a password that consists of only grid positions that fall within a 3x3 grid, we find 7% of all passwords captured to fall under this category.

In summary, the statistics for the five identified patterns are given in Table II. The statistics shows that the number of hotspots significantly decreases from first enrolment (28%) to second enrolment (10%) – see Fig. 4. A similar significant drop is seen in the statistics for the Colour pattern where the pattern is observed for 48% of password selections for the first enrolment and only 19% for the second enrolment. However, for other patterns, such as Lines, 3x3 and Border patterns there is no significant decrease in the observation of the patterns between first and second enrolment. This seem to signify that users change their behaviour only on the patterns that was specifically pointed during the education session between the two enrolments. That is, users tend not to generalize the existence of patterns and only try to avoid hotspots because that pattern was explicitly pointed out to them.

Overall 61% of first enrolment passwords fall into one of the five patterns identified. Even after user education the second enrolment still contain 46% passwords conforming to the identified patterns.

The remainder of yjr passwords, not fitted to the already mentioned patterns are *not* random. There are other patterns that were identified, but with much lower frequencies. For example about 4% of the passwords consist of line segments similar to Fig. 6 (bottom-left), consisting of 2 or more linear parts. The pattern represented in Fig. 6(top-right) consists of a pattern such as zig-zag or double-lines, but started at a hotspot; 2.4% of passwords have this pattern.

TABLE II
PASSWORD PATTERN STATISTICS

Pattern	1st Enrolment	2nd Enrolment	Combined
Lines	26%	27%	26%
Hotspot	28%	10%	19%
3x3	7	8%	7%
Border	6%	6%	6%
Colour	48%	19%	33%

IV. LIMITATIONS

The study itself was focused on the gathering of qualitative information on password patterns. This is a relatively rare study type for GPs. Most researchers select quantitative studies, typically involving student subjects. Here we attempted to understand GP pattern selection not only by carefully investigating the passwords, but also by interviewing subjects as to what informed their password selection choices.

V. FURTHER WORK

This publication is the third in a series of publications that investigate GPs from different angles using qualitative methods. In the first study [37], the characteristics of GPs were investigated in the context of length and strength. It was shown that in conventional passwords there is character re-use, but in GPs, the re-use of symbols or positions on the image is significantly lower than what is statistically expected. The second study [36] investigated user perceptions regarding graphical passwords, concluding that users in general are still apprehensive to use such technologies for enterprise-level security, such as for authentication during financial transactions. This paper investigated the pattern-richness of GPs.

The use of GPs is now main stream in the sense that they are used widely in device security such as Android pattern unlock. There are, however, significant gaps in understanding what is required to make GPs operational in an enterprise environment.

In addition, since we have shown in this paper that user education has a appreciative effect on behaviour such as hotspot selection, we know that there is still a significant gap between user awareness of security in both conventional and graphical passwords.

VI. CONCLUSION

In this paper we set out to investigate user patterns in graphical passwords by using qualitative methods. We interviewed participants and asked them to enrol with five different images. After asking users for the the reasoning behind their selections and educating the participants on the dangers of hotspots, the users were asked to re-enrol with the same five images.

We find that although there is a significant drop in the number of hotspot passwords, there is still a appreciable pattern-based bias within the second enrolment password set. In particular we find that even after user education, 46% of the second enrolment passwords conform to the five identified categories.

References

[1] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[2] G. Blonder, "Graphical password. us patent 5559961, lucent technologies," *NJ: Murray Hill*, 1995.

[3] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Information Security and Privacy*. Springer, 1998, pp. 403–414.

[4] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin *et al.*, "The design and analysis of graphical passwords." in *Usenix Security*, 1999.

[5] S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," in *People and Computers XIVUsability or Else!* Springer, 2000, pp. 405–424.

[6] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in *USENIX Security Symposium*, vol. 9, 2000, pp. 4–4.

[7] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.

[8] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," *Journal of Computer Security*, vol. 19, no. 4, pp. 669–702, 2011.

[9] H. Tao, "Pass-go, a new graphical password scheme," Master's thesis, University of Ottawa, 2006.

[10] P. Dunphy and J. Yan, "Do background images improve draw a secret graphical passwords?" in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 36–47.

[11] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," *NIST Report: NISTIR 7030*, 2003.

[12] P. Bao, J. Pierce, S. Whittaker, and S. Zhai, "Smart phone use by non-mobile business users," in *Proceedings of the 13th international conference on human computer interaction with mobile devices and services*. ACM, 2011, pp. 445–454.

[13] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." *WOOT*, vol. 10, pp. 1–7, 2010.

[14] F. Alt, S. Schneegass, A. S. Shirazi, M. Hassib, and A. Bulling, "Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2015, pp. 316–322.

[15] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 161–172.

[16] H. Gao, X. Liu, S. Wang, and R. Dai, "A new graphical password scheme against spyware by using captcha." in *SOUPS*, 2009.

[17] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, "Captcha as graphical passwordsa new security primitive based on hard ai problems," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 6, pp. 891–904, 2014.

[18] S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, "A novel image-based implicit password authentication system (ipas) for mobile and non-mobile devices," *Mathematical and Computer Modelling*, vol. 58, no. 1, pp. 108–116, 2013.

[19] A. Juels and R. L. Rivest, "Honeywords: Making password-cracking detectable," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 145–160.

[20] B. B. Zhu, J. Yan, D. Wei, and M. Yang, "Security analyses of click-based graphical passwords via image point memorability," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 1217–1231.

[21] D. Florêncio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 657–666.

[22] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Computer security applications conference, 21st annual*. IEEE, 2005, pp. 10–pp.

[23] S. Man, D. Hong, and M. M. Matthews, "A shoulder-surfing resistant graphical password scheme-wiw." in *Security and Management*. Citeseer, 2003, pp. 105–111.

[24] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*. ACM, 2006, pp. 177–184.

[25] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *Cyberworlds (CW), 2010 International Conference on*. IEEE, 2010, pp. 194–199.

[26] Y.-L. Chen, W.-C. Ku, Y.-C. Yeh, and D.-M. Liao, "A simple text-based shoulder surfing resistant graphical password scheme," in *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on*. IEEE, 2013, pp. 161–164.

[27] A. S. Gokhale and V. S. Waghmare, "The shoulder surfing resistant graphical password authentication technique," *Procedia Computer Science*, vol. 79, pp. 875–884, 2016.

[28] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in *USENIX Security Symposium*, vol. 13, 2004, pp. 11–11.

[29] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 1–12.

[30] P. C. van Oorschot and J. Thorpe, "On predictive models and user-drawn graphical passwords," *ACM Transactions on Information and system Security (TISSEC)*, vol. 10, no. 4, p. 5, 2008.

[31] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, pp. 387–398, 2009.

[32] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 162–175.

[33] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 20–28.

[34] J. S. Vorster, "A Framework for the Implementation of Graph-

ical Passwords," Master's thesis, University of Liverpool, 12 2014.

[35] S. Peach, J. Voster, and R. Heerden, "Heuristic attacks against graphical password generators," in *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa*, 2010, pp. 272–284.

[36] J. S. Vorster and R. van Heerden, "A study of perceptions of graphical passwords," *Journal of Information Warfare*, vol. 14, no. 3, 10 2015.

[37] ——, "Graphical passwords: A qualitative study of password patterns," in *The Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015)*, L. Armistead, Ed. Academic Conferences Limited, February 2015, pp. 375–383.