Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)

Heuristic Attacks Against Graphical Password Generators

S. Peach, J. Vorster and R. van Heerden

Council for Scientific and Industrial Research
e-mail: Speach@csir.co.za; jvorster@csir.co.za; rvheerden@csir.co.za

Abstract

In this paper we explore heuristic attacks against graphical password generators. A new trend is emerging to use user clickable pictures to generate passwords. This technique of authentication can be successfully used for - for example - operating system authentication. We report on the development of a generic tool for password generation using such a graphical click-driven interface. This stand-alone tool can be used for generating passwords on the fly. We describe the approach and the usability of such a project. The project is available as an open-source project. Next we investigate heuristic attacks against such generated passwords. By using a classifier methodology it is possible to develop specific attack-scenarios based on the category. Specific heuristic attacks are used to reduce the key-space such that brute-force cracking approaches become feasible. We report on these heuristic attacks and their success. Lastly we give criteria for images that should be used in such password generation applications to avoid these types of heuristic attacks.

Keywords

Graphical Passwords, Heuristic Password Attack, Password Cracking, Graphical Password Generator

1. Introduction and Background

Keyboard-based passwords have been the standard for many years. However, recently new passwords schemes have emerged. From audio-based schemes (Chiasson et al. 2008) to graphical based schemes.

Almost all hardware applications (ATM, PDAs, PCs, etc.) of data-devices now have some form of input device that allow for point-selection – stylus in PDAs, mouse on PCs and touch screens at ATMs. This ubiquity of graphical user interfaces coupled with the access to the above mentioned input devices have created the ideal conditions for a change in the authentication mechanisms traditionally used. In particular, this has enabled the development of graphical user authentication techniques (Blonder 1995, Dhamija, Perrig 2000).

Graphic password schemes have many advantages over normal password schemes in applications that provide mouse, touch-screen or stylus input. The range of applications of these types of schemes varies greatly, from hand-held devices such as PDAs to internet applications such as bank-authentication. This type of authentication is of particular interest in applications without keyboard input.

One of the advantages of such an authentication scheme is that the potential exists for such passwords to be much more secure than conventional keyboard based passwords. In a well referenced paper Madigan (1983) has shown that we are better at remembering pictures than words. The premise of graphical authentication schemes are therefore based on this and later research and aim to improve the strength of passwords by using human memory systems that are stronger, such as picture memory, as shown by Madigan.

Suo et.al. (Suo et al. 2005) surveyed a large number of different graphical password schemes. They conclude, though guardedly, that graphical passwords seem more secure than conventional passwords, but also point out that this has not been studied sufficiently.

Wiedenbeck et.al. (Wiedenbeck et al. 2005) conducted a longitudinal evaluation of the PassPoints graphical password system. They point out that that key-space for graphical passwords is significantly larger than alphanumeric alphabets, thus allowing for either fewer clicks to achieve the same security level, or a more secure password.

On the disadvantage side, graphical schemes have the potential for shoulder-surfing attacks. Some authors have proposed schemes to overcome spying attacks (Komanduri, Hutchings 2008).

Another proposal was the use of user-drawn pictures as graphical passwords. The design of such a scheme was discussed by Jermyn et.al. (1999). Oorschot and Thorpe (2008) however built a number of predictive models to attack this password scheme, they also made a number of suggestions (2004) on how to improve these "Draw-a-secret" approaches.

2. Face Based Graphical Password Schemes

Face based graphical password software has been implemented commercially – see for example PassFace (Brostoff, Sasse 2000, Valentine 1999). In all the implementations of face-based authentication, the user is presented with a number of faces – say nine – and then has to select the specific face that forms part of the "password" faces while ignoring the other faces what was randomly selected from a database of faces. The user has to repeatedly select the correct face in a number of rounds – say five. This scheme was studied by Davis et. al. (2004) using a number of students. In their scheme users were presented with a 3x3 image of nine faces from which they had to select the correct face in four rounds.

Let's analyze the security of such a configuration. If the user is presented with n faces to choose form and the authentication lasts for m rounds, then the total number of passwords than can be generated using this scheme is:

$$n^m$$

and the probability of guessing the correct password by randomly selecting a face on each round would then be

P(randomly guessing the correct password) = (1/n)m

Then the number of attempts before we stumble upon the password would be 1/P.

Processing the numbers for the Davis experiment (n = 9, m = 4) we find that

P(randomly guessing Davis experiment password) = 1.524 x 10-4

and thus the number of attempts needed to brute-force crack this scheme is: 6561.

This scheme is does not present sufficient security. Davis however acknowledges the security limitations of the experiment. Improving the security of such a scheme can be done in two ways, firstly increasing the number of faces shown on every trail, and secondly increasing the number of trails. With a 5x5 grid the brute-force number for m=4 trails is: 390625. This is still not a sufficient level of security.

A human's capability to spot the correct face within a sea of more than 25 faces (5x5) becomes more difficult, 36 faces with a 6x6 grid and just under 50 faces with a 7x7 grid. It seems from the complexity of searching for the correct face that a 5x5 grid is possibly the maximum, although we could not find any studies that focused on this specific aspect and therefore it is difficult to put an upper limit on the number of faces that could be displayed with this specific scheme.

It does seem that this scheme has some limitations. Increasing the number of rounds is another option, but this has serious time implications for logging in. A user would not want to spend a long time trying to log in by going though a large number of rounds. So increasing the number of rounds will have an impact on the user's ability to be authenticated quickly. This will have a direct impact on the user's experience of such a system.

However, there is another attack on this type of authentication scheme that is possible. A malicious user may, over a long period, attempt to authenticate by impersonating a legitimate user. Such a cracker would provide the required credentials to start the authentication process – usually the user name, which is publicly known or easily gathered. Then, on every request that the system makes for a password the cracker captures the images provided – screen capture, or digital camera. The key to cracking the authentication scheme is in realizing that the authentication system provides the cracker with knowledge about the user's password. One of the n images shown is the correct one. By repeating the image-capturing process over a number of days – so that the user is not logged out, enough information may be gathered to safely and easily crack this type of authentication process.

There are two ways for the authentication process to handle a false face selection: stop after the first incorrect answer and declare an invalid login, or stop after all m rounds have been completed.

In the first instance the cracker can only capture one image on every try; however, he also gains the knowledge that the image he selected was not the correct one, thus leaving n-1 faces as the potentially correct face.

In the second scheme, that may sound more secure, the system actually gives away m images and thus m pieces of information about the user password.

The way the authentication systems handles failure is also important. Say a user enters correct credentials and is presented with an image. If the user now shuts down the computer, reboots it, or simply exists the login system, does the system log it as a login attempt? If it does not, then a cracker may repeatedly go through this initial process, each time receives an image from the authentication system that contains a face that is part of the user's password. Thus in this way, within a very small number of tries a cracker may be able to figure out what the user's pass-faces are.

We therefore suggest that this type of password scheme is not secure against a sophisticated cracker.

3. Image Based Passwords: The Human Factor

As mentioned above Davis et. al. (2004) studied a face-based authentication system. Their main aim was not to verify the inherent security of the scheme based on the analysis we did above, but rather to understand what type of pass-faces the users would chose and to study the inherent patterns within these choices.

In the study users were requested to set an initial sequence of faces that would be used as the pass-face sequence. Within these images the researchers imbedded the image of a male and female model on each of the initial faces from which the user had to choose pass-face. Their results showed significant bias especially on the male set of users for selecting the model. The results (Davis, Monrose & Reiter 2004) are shown below:

Pop.	Female Model	Male Model	Typical Female	Typical Male
Female	40.0%	20.0%	28.8%	11.3%
Male	63.2%	10.0%	12.7%	14.0%

Table 1: Gender and attractiveness selection in face-based authentication

Pop.	Asian	Black	White
Asian Female	52.1%	16.7%	31.3%
Asian Male	34.4%	21.9%	43.8%
Black Male	8.3%	91.7%	0.0%
White Female	18.8%	31.3%	50.0%
White Male	17.6%	20.4%	62.0%

Table 2: Race selection in face-based authentication

The above two results from Davis gives further support to the idea that these types of pass-face authentication schemes may be vulnerable to attack based on human factors.

The inherent biases shown in the tables and discussed by Davis can be effectively used for guessing pass-images. A possible future research topic could be the construction of Markov models for pass-face guessing based on statistics of this nature.

4. Experimental Setup

We developed a graphical authentication system based on images. Users authenticate by selecting specific grid-spots within the image. A user may select as many (or few) points as they wish, with no limitations. A total of 22 people participated, each using all 4 images. Users were asked to choose a pass-phrase which they would be able to repeat.

The hypothesis is that users will select very specific points of interest such as faces (Figure 1), sharp points (Figure1, Figure 3) or facial features such as eyes and nose (Figure 4) and we were interested to see what users will select when faced with a very limited number of such interesting points (Figure 2 and Figure 3).

Figure 1: Shopping Centre

Figure 2: Sailboat

Figure 3: Kitten

Figure 4: Lena

Considerable effort was put into image selection. Each image was chosen to verify a specific part of the hypothesis.

A large number of people were asked to select a pass-phrase based on each of the images above. Although we are not interested in how well people will remember these passwords, rather we are interested in their initial selection of points to form the passwords. Each user had to generate a pass-phrase for each of the images. The click-points were stored in a database for later analysis.

5. Results and Discussion

The data from all the passwords were gathered and centralized. Each password consisted of a number of mouse-clicks. We stored the specific points where the mouse was clicked as well as the block where the click occurred. Thus we are able to show the exact location where the user had selected a point. A number of passwords are shown in Figure 5, where each white dot represents one mouse-click.

The kitten picture (Figure 3) was chosen because of the low scene complexity, thus forcing the user to either stick with a small number of hot-spots, or choose another point selection scheme.

Therefore the user would be forced to select from a very small number of points that are easily memorized – such as tail-point, ears, nose, etc.

Figure 5: Lena showing the click-points for 20 passwords

We found that password length did not vary much. The shortest password was 5 clicks and the longest 14 clicks which is an outlier since the second longest is 8 clicks. However, the average password length as consistent over the pictures with an average of 6.38 clicks.

Image	Shortest	Longest	Average
Shopping	5	8	6.21
Sailboat	5	8	6.11
Lena	5	14	6.70
Kitten	5	10	6.48
Overall	5	14	6.38

Table 3: Statistics on password length per image

After data-analysis we found that passwords generated can be broadly classified into five categories:

Category	Description	Example
Picture Independent	The click pattern is independent of the picture.	Figure
Picture Offset	The click pattern forms a distinct pattern that could have been picture independent, but the user chose a hotspot on the picture as an offset for the pattern.	Figure
Picture Hot-points	The click pattern is highly dependent on the image and follows some pattern such as tail, nose, mouth.	Figure
Hybrid	Some hybrid of an image independent pattern and offset pattern.	Figure
Pseudo-random	The researchers could not classify the pattern as any of the above.	Figure

Table 4: Categories for click pattern classification

We found that the picture independent patterns are strongly user-bound, that is, if a user chose such a pattern for one image, that user would also use such a pattern on subsequent images. Furthermore, we found that a specific user would often – about one-third of the time – repeat the pattern on more than one of the images.

The second class of patterns is similar to the independent pattern, but the user chose to offset the pattern by using a hotspot on the image. The pattern displayed in Figure shows this clearly where the specific password is two rows of three blocks, but placed on the body of the kitten.

The third category of patterns we found is based on hotspots as shown in Figure. In this category the user selected points that form distinct features of the image. In this case the point of the kitten's tail, ears, nose and the hedgehog's front spike-points and nose.

The fourth category is a hybrid pattern consisting of an image independent part combined with an image offset pattern. An example of such a pattern is shown in Figure.

The final click pattern category is a catch-all category for patterns that the authors could not classify either by finding an obvious pattern or algorithm for its generation. In future work we could enquire from the users what the selection strategy they used, especially for users where a clear-cut classification was not possible.

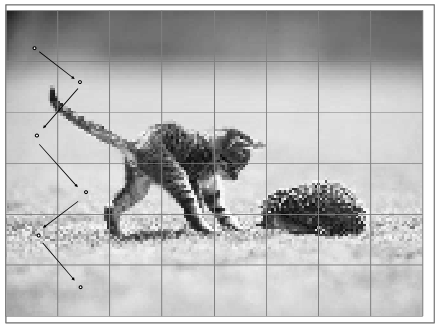

Figure 6: Pattern password – independent of picture

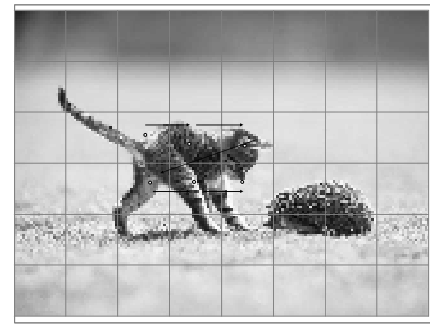

Figure 7: Pattern password – dependant on picture hotspot offset

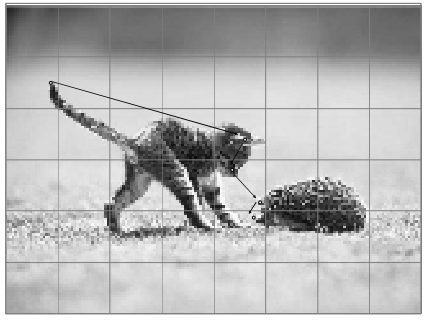

Figure 8: Picture hotspot pattern

Figure 9: Hybrid pattern

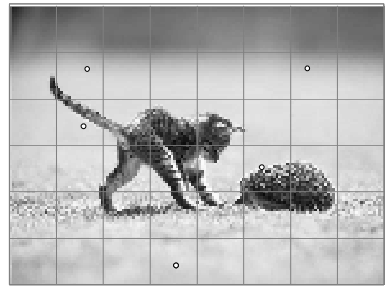

Figure 10:Pseudo-random pattern

From a cracking point of view the first two pattern categories (picture independent pattern and picture offset pattern) can be categorised together as some form of pattern with an offset. We found that a significant number (45%) of passwords fall into the first two categories. Table 5 below shows the percentage of passwords that fall into these two categories, for each picture.

The user community that took part in this study are used to entering passwords for various systems such as email clients. Although it could not be verified we speculate

that the high number of patterns is a reflection of the password selection strategy that these users use for letter-based passwords. A study into such a correlation would be valuable contribution to understanding how users select graphic based passwords.

Image	% of passwords
Shopping	47%
Kitten	43%
Sailboat	44%
Lena	50%

Table 5: Percentage of passwords that have a distinct pattern – Pseudo independent of the image

The kitten picture was selected specifically because it would force the user into a very limited number of options in terms of easily remembered points on the image to select as pass-points. An analysis of the blocks chosen by the users reflect his clearly. In Figure 11 below we see the highlighted blocks are those blocks that were not used for any of the passwords. That is, these blocks do not form part of any password. The next figure - Figure 13- shows the unused blocks after the independent patterns and image offset patterns were removed.

The initial image was broken up into a 6x8 grid, this yielded 48 blocks to select from. The average password length was shown to be 6.38 clicks. Thus we can compute the average password strength as in terms of bit-representation as

$$486.38 = 235.63 \ ,$$

so that any given average password, if selected from random blocks will have a 36 bit strength. This is not significant, easily cracked using even modest equipment such as PCs. However, this study was not into the direct strength of the passwords, but rather into the user selection and the human factors in password selection. However, we will use this number - 36 bits – as a reference point to show the effect of the human factors on graphical based password selection.

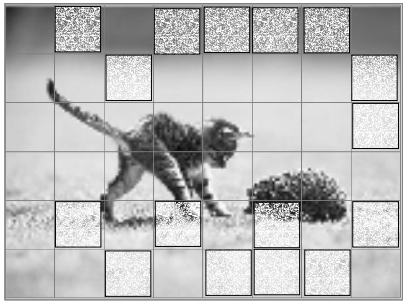

Figure 11:Kitten - showing blocks that were not used

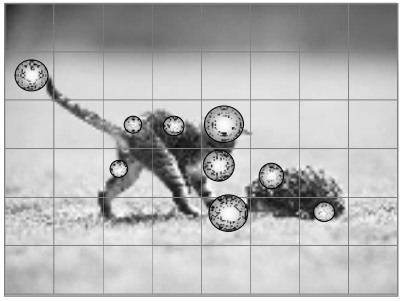

Figure 12:Kitten – showing hotspots

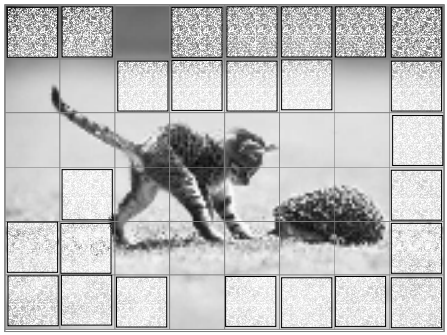

Figure 13: Kitten - showing blocks that was not used for any passwords – Pseudo-random and Hotspot patterns only

Statistical analysis show that for most of the pictures more than 80% of the blocks are used, with the kitten picture at 70%. The kitten picture was selected to have little detail and therefore we expect the lower number. However, if we remove the picture independent patterns and the picture offset patterns from the analysis set, the picture changes significantly. As shown in Figure, a significant portion of the image is not used, and therefore a brute force approach to cracking passwords generated form these types of images becomes feasible even with a much higher block rate per image.

In this particular kitten image we find that after removal of the above mentioned patterns that 24 blocks remain, that is 50% of the original blocks. Now re-computing the password bit-length gives

246.38 = 2 29.25,

thus a bit-length of only 29. This yields a 7 bit reduction in the complexity of cracking the password.

This is however the worst-case scenario for a cracker. We found that most of the passwords use the hotspots as indicated in Figure. In this future the size of the circles indicate the relative number of points that fall in that block and the relative position in the block where the most clicks occurred. This account for 83% of the passwords that fall in this selection categories (hotspot patterns and pseudo-random patterns). To recap, 43% of passwords were pattern based and we removed them from the analysis set, that leaves 47% passwords. Of these 47% we found that 83% can be accounted for by Figure which consists of nine blocks, 18.75% of the image.

Thus we will be able to crack 0.47*0.83 = 39% of all the passwords by using 18.75% of the blocks, yielding password strength of

9 6.38 = 2 20.22

Thus a bit-length of only 20. This shows that a wrong selection of picture for the generation of passwords can have a significant impact on the security of such a system.

The other images do show more complex password behaviour, as shown in the images below.

Figure 14: Shopping – showing hotspots

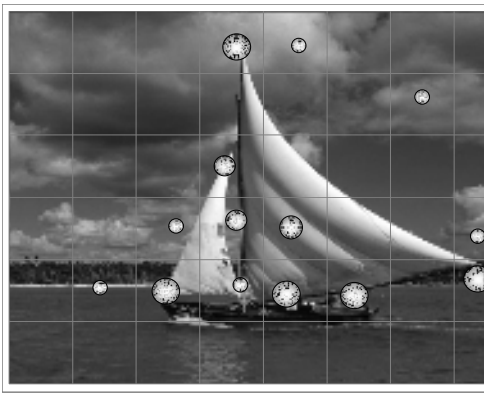

Figure 15: Sailboat – showing hotspots

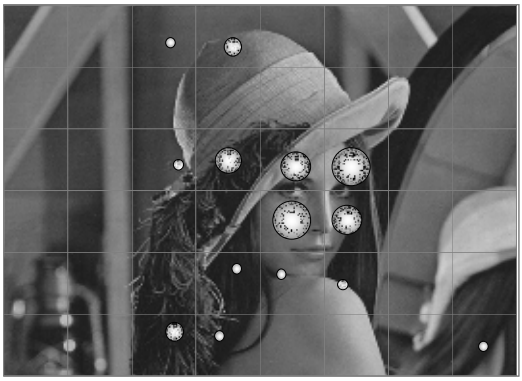

Figure 16: Lena – showing hotspots

The analysis given thus far coupled with the data we gathered now suggests a number of attack methods that could be used against graphical passwords.

For the first two categories – picture independent patterns and picture offset patterns a direct pattern generation cracking scheme analogue to keyboard patterns would be effective. This approach to cracking conventional passwords has been investigated already; see for example (Van Heerden, Vorster 2009). Also, statistical attacks such as the use of Markov models would be an effective method for controlling the search space, similar to the approaches followed by van Heerden et.al. (2008) that used Markov models to optimize the search space for conventional passwords.

Passwords generated by high usage of hit-spots (Figures 12, 14-16) has a number of approaches that may be used. Thorpe and Oorschot (2007) showed that human-seeded hot-spot identification is an effective method for attacking these password choices. Their simple approach showed that between 10% and 20% and as high as 30% of passwords could be cracked using this method.

Hybrid passwords are more difficult as the pattern-shift is not predictable. Pseudo-random patterns are also difficult to predict by nature. These two categories of passwords will be the most difficult to crack. From a user-perspective the latter is not usable since it is difficult to remember some random password, however, the first approach may give a workable approach to improving graphical based passwords.

6. Conclusion and Further Work

In this paper we set out to show that graphical based passwords are vulnerable to attacks using human factors.

We showed that more than 40% of the users we surveyed used patterns that are either independent of the image of a pattern that uses only one offset point in the image. These patterns cannot be cracked using hot-spot approaches, but they can be attacked using conventional keyboard pattern and Markov model approaches.

A significant portion – 39% - of passwords were hot-spot based. These passwords have a significant disadvantage and could be attacked in a number of ways, of which human-seeded hot-spots is one.

The remaining 21% of passwords are more difficult to crack. However, the conclusion that plausible attack methods exists for about 80% of graphic based passwords is a matter of concern.

A number of potential research topics has emerged from this work. The use of Markov models for the prediction of face-based authentication based on the statistics from Davis et.al. (2004) would further improve the human factors approach to attacks on these schemes.

The pseudo-random patterns that were identified could fall into two possible categories, truly random, and thus impossible to predict, or alternatively based on some form of unidentified pattern. A study into pseudo-random patterns via interviews with users that select such passwords may be plausible approach to further taxonomize graphical passwords.

7. References

Blonder, G.E. (1995), Graphical Password, US Patent 5559961, Lucent Technologies, Inc., Murray Hill, NJ, August 30, 1995.

Brostoff, S. & Sasse, M.A. (2000), "Are Passfaces more usable than passwords: A field trial investigation", People and Computers XIV-Usability or Else: Proceedings of HCI, pp 405.

Chiasson, S., Forget, A. & Biddle, R. (2008), "Accessibility and Graphical Passwords", Symposium On Accessible Privacy and Security (SOAPS), July 2008.

Davis, D., Monrose, F. & Reiter, M.K. (2004), "On user choice in graphical password schemes", Proceedings of the 13th conference on USENIX Security Symposium-Volume 13, USENIX Association, pp 11.

Dhamija, R. & Perrig, A. (2000), "Deja vu: A user study using images for authentication", Proceedings of the 9th conference on USENIX Security Symposium-Volume 9, USENIX Association, pp 4.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. & Rubin, A.D. (1999), "The design and analysis of graphical passwords", Proceedings of the 8th conference on USENIX Security Symposium-Volume 8, USENIX Association, pp 1.

Komanduri, S. & Hutchings, D.R. (2008), "Order and entropy in picture passwords", Proceedings of graphics interface 2008, Canadian Information Processing Society, pp 115.

Madigan, S. (1983), "Picture memory", Imagery, memory and cognition, pp 65–89.

Oorschot, P. & Thorpe, J. (2008), "On predictive models and user-drawn graphical passwords", ACM Transactions on Information and System Security (TISSEC), vol. 10, no. 4, pp 5.

Suo, X., Zhu, Y. & Owen, G.S. (2005), "Graphical passwords: A survey", 21st Annual Computer Security Applications Conference, (ACSAC)Citeseer, pp 463–472.

Thorpe, J. & van Oorschot, P. (2007), "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords", The 16th USENIX Security Symposium.

Thorpe, J. & Van Oorschot, P. (2004), "Towards secure design choices for implementing graphical passwords", 20th Annual Computer Security Applications Conference, pp 50.

Valentine, T. (1999), "Memory for Passfaces TM after a long delay", Technical Report, Goldsmiths College University of London, 1999.

van Heerden, R. & Vorster, J. (2008), "Using Markov Models to Crack Passwords", The 3rd International Conference on Information Warfare and Security: Peter Kiewit Institute, University of Nabraska, Omaha USA: 24-25 April 2008, Academic Pub., pp. 387.

Van Heerden, R. & Vorster, J. (2009), "Statistical analysis of large passwords lists, used to optimize brute force attacks", The 4th International Conference on Information Warfare and Security: Council for Scientific & Industrial Research, South Africa: 26-27 March 2009.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. & Memon, N. 2005, "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp 102-127.