Persuasive Cued Click-Points: An Implementation of a Knowledge-Based Authentication Mechanism

Mr. N.Gobinathan[1], Mr.L.Prakashkumar[2] and Mr. R.Anwer Hussain[3]

[1]Assistant Professor of Computer Science, V.R.S. College of Engineering and Technology, Arasur, Villupuram.

[2]Final Year Computer Science, V.R.S. College of Engineering and Technology, Arasur, Villupuram.

[3]Final Year Computer Science, V.R.S. College of Engineering and Technology, Arasur, Villupuram.

Abstract

Our paper presents an integrated evaluation of the Persuasive Cued Click-Points graphical password scheme, including usability and security evaluations, and implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points.

1.Introduction

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember.

A password authentication system should encourage strong passwords while maintaining memorable. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password—a feature lacking in most schemes.

We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) and conducted user studies evaluating usability and security. This paper presents a consistent as simulation of earlier work and two unpublished web studies, reinterprets and updates statistical analysis incorporating larger data sets, provides new evaluation of password distributions, extends security analysis including relevant recent attacks, and presents important implementation details. This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues, to advance understanding as is prudent before practical deployment of new security mechanisms.

Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks Graphical passwords offer another alternative, and are the focus of this paper.

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information.

1.1 Click Based Passwords

In Pass Points, passwords consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To login, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable, security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints passwords. Users also tend to select their click-points in predictable patterns (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat.

A precursor to PCCP, Cued Click Points was designed to reduce pattern sand to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point (Fig.1), creating a path through an image set. Users select their images only to the extent that their click-point determines the next image Creating a new password with different click-points results in a different image sequence. The claimed advantages are that password becomes a true cued-recall scenario, where in each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

1.2 PersuasiveTechnology

Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

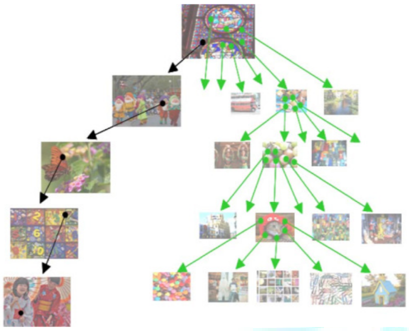

Fig.1.A user navigates through images to form a CCP password. Each click determines the next image

2.Persuasivecued Clickpoints

Visual attention research shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue. Davis et al. suggest that user choice in all types of graphical passwords is in advisable due to predictability.

By adding a persuasive feature to CCP PCCP encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport (seeFig.2). The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. The viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this high-lighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

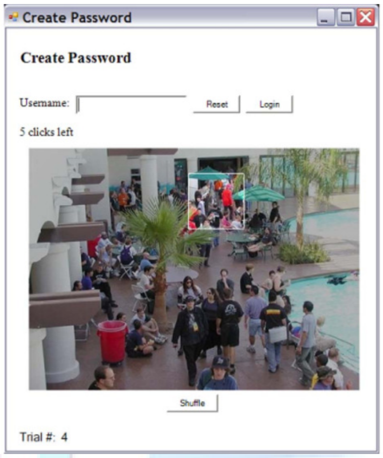

Fig.2. PCCP Create Password interface

3. Description of User Studies Usability Evaluation

We consider the following performance measures for memorable and usability: login and recall success rates, times for password creation, login, and recall, and the effect of shuffling on success rates. Logins occurred during the initial lab session and tested shorter term memorable, while recalls occurred either at home or during a second lab session and tested long-term memorable. Where appropriate, the same measures are included for the PassPoints, CCP, and Text studies. The studies were conducted over a few years and the analysis evolved as we gained more experience. In this paper, results have been recalculated using the same process, to allow for more accurate comparison. As such, the numbers may vary from earlier publications.

3.1 Success Rates

Success rates are reported on the first attempt and within three attempts. Success on the first attempt occurs when the password is entered correctly on the first try, with no mistakes or restarts. Success rates within three attempts indicate that fewer than three mistakes or restarts occurred. Mistakes occur when the participant presses the Login button but the password is incorrect. Restarts occur when the participant presses the Reset button midway through password entry and restarts password entry. Restarts are analogous to pressing delete while entering text passwords, except that PCCP's implicit feedback helps users detect and correct mistakes during entry.

3.2 Password Entry Times

Times are reported in seconds for successful password entry on the first attempt. For login and recall, we also report the "entry time": the actual time taken from the first click-point to the fifth click-point. The analogous measure was not recorded for text passwords. During password creation, this can partially be explained by participants who used the shuffle mechanism repeatedly. During recall, this may be because PCCP participants had to recall different passwords (since by design, it is impossible to reuse PCCP passwords), whereas over half of Text participants reused passwords or had closely related passwords, suggesting a reduced memory load.

3.3 Varying System Parameters Success Rates

Success rates were very high for login; participants could successfully login after a short time regardless of number of click-points or image size. Success rates after two weeks were much lower in all conditions, reflecting the artificial difficulty of the memory task—recalling six passwords created in a short time and not accessed for two weeks. The L7 condition had the lowest success rates, suggesting that passwords using large images and seven click-points combined were most difficult.

3.4 Shuffles

During password creation, PCCP users may press the shuffle button to randomly reposition the viewport. Fewer shuffles lead to more randomization of click-points across users. The shuffle button was used moderately.

4. Analysis of Password Distributions

4.1 Click-Point Clustering

To analyze the randomness and clustering of 2D spatial data across users, we turned to point pattern analysis commonly used in biology and earth sciences. The analysis used at, a spatial statistics package for the programming language.

4.2 Varying Number of Click-Points

As detailed in an earlier paper, we examined the effects of the number of click-points on clustering on the PCCP 2wk data.

4.3 Varying Image Size

We also used the PCCP 2wk data to examine clustering due to image size .Fisher's exact test shows a significant difference (p ¼0:002), indicating significantly less clustering for larger images.

IJREAT PRDG

4.4 Hotspot Coverage

We summarize the hotspots per image using cumulative frequency distributions for the 17core images. The distributions contain all user-chosen click-points for the given scheme for passwords that were, at minimum, successfully reentered at least once during login. In other words, all click-points in the data set are represented (including "hotspots" consisting of only one user-chosen click-point).

Security

We next discuss PCCP's resistance to standard security threats: guessing attacks and capture attacks.

Guessing Attacks

The most basic guessing attack against PCCP is a brute-force attack, with expected success after exploring half of the password space (i.e., with a theoretical password space of2^{43}, success after 2^{42} guesses). However, skewed password distributions could allow attackers to improve on this attack model. Section6 examined the password distributions based on several characteristics. We now consider how these could be leveraged in guessing attacks.

4.5 Pattern-Based Attack

One of the proposed attacks on PassPoints is an automated pattern-based dictionary attack that prioritizes passwords consisting of click-points ordered in a consistent horizontal and vertical direction (including straight lines in any direction, arcs, and step patterns), but ignores any image-specific features such as hotspots. The attack guesses approximately half of passwords collected in a field study on the Cars and Pool images (two of the17core images) with a dictionary containing 2^{35} entries, relative to a theoretical space of2^{43}.

Given that PCCP passwords are essentially in distinguishable from random for click-point distributions along the x-and y-axes, angles, slopes, and shapes (see technical report), such pattern-based attacks would be ineffective against PCCP passwords.

4.6 Summary of Password Distributions

Analysis of click-point clustering showed that PCCP had the least clustering of click points across different users. Similarly, hotspot analysis showed that PCCP had the flattest click-point distribution and was least likely to contain hotspots when compared to CCP and PassPoints. In tests of numerous spatial relationships and patterns, we found no significant differences between PCCP and what is expected to occur by chance. And finally, color analysis showed that users did not choose click-points within passwords based on color of images must be determined and each relevant image collected, making a customized attack per user. An online attack could be the by limiting the number of in correct guesses per account.

To explore an offline version of this attack, assume in the worst case that attackers gain access to all server-side information: the user name, user-specific seed, image identifiers, images, hashed user password, and corresponding grid identifiers. The attacker determines the first image I_1 from the available information. Hotspot analysis identifies the center of the largest hotspot on I_1.The next image

I_2 is predicted based on I_{1}'s hotspot and the user-specific seed which determines the image mapping. In this way, a password guess contains the largest hotspot on each predicted image. The same process could be used to determine passwords using five subsets of popular hotspots. The resulting dictionary would grow combinatorial based on the number of hotspots followed at each stage. Because each user password in PCCP involves different images, it is difficult to collect enough statistical information in an experimental setting for meaningful hotspot analysis.

We next consider a second hotspot attack strategy under the same assumption of all server-side information being known, and in this case, consider the level of effort required for a three percent chance of guessing a target password. With the basic configuration of1 9 19 pixel tolerance squares, and 451331 pixel images, there are approximately 400 tolerance squares per image. If no hotspots exist and there are no patterns (i.e., if random and independent click-points are chosen), each tolerance square has an equal 1=400 chance of being part of the user's password.

Capture Attacks

Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user- entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge-based authentication schemes), capturing one login instance allows fraudulent access by a simple replay attack. We summarize the main issues below; detailed discussion is available elsewhere.

Shoulder Surfing

All three cued-recall schemes discussed (PCCP, CCP, and PassPoints) are susceptible to shoulder surfing although no published empirical study to date has examined the extent of the threat. Observing the approximate location of click- points may reduce the number of guesses necessary to determine the user's password. User interface manipulations such as reducing the size of the mouse cursor or dimming the image may offer some protection, but have not been tested. A considerably more complicated alternative is to make user input invisible to cameras, for example, by using eye tracking as an input mechanism.

4.7 Malware

Malware is a major concern for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

4.8 Social Engineering

For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password insufficient, detail. One preliminary study suggests that password sharing through verbal description may be possible for PassPoints. For PCCP, more effort may be required to describe each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords.

PCCP and CCP have a security advantage over PassPoints: an attacker launching a phishing attack would need to retrieve many images from the server instead of only one. With a man-in-the-middle (MITM) attack, only one image per click-point would need to be retrieved, since the correct image would be identified by the legitimate website when the user's click-point is entered. However, attackers who collect the images beforehand would need together all of them in order to display the correct next image when the user enters a click-point. Attackers who make assumptions about likely hotspots and only collect the corresponding images risk missing images if the user clicks elsewhere. Although social engineering remains a threat with PCCP, attacks require significantly more effort and have a lower probability of success than for text passwords or PassPoints.

Summary of Security Analysis

Given that hotspots and click-point clustering are significantly less prominent for PCCP than for CCP and PassPoints, guessing attacks based on these characteristics are less likely to succeed. Taking into account PCCP's sequence of images rather than a single image offers further reduction in the efficiency of guessing attacks. For capture attacks, PCCP is susceptible to shoulder surfing and malware capturing user input during password entry. However, we expect social engineering and phishing to be more difficult than for other cued-recall graphical password schemes due to PCCP's multiple images.

Relevant Implementation Issues

The following discusses two prototype implementations of PCCP and highlights issues relevant for a best practice implementation. The first prototype, intended for experiments only, included design decisions which facilitated data gathering but would not be advisable in actual deployment.

Discretization

Discretization of click-points allows for approximately correct click-points to be accepted by the system without storing exact click-point coordinates in the clear. Our second prototype implemented Centered Discretization, wherein an invisible discretization grid is over laid on to the image, dividing the image into square tolerance areas, to determine whether a login click-point falls within the same tolerance area as the initial click point. For each click-point, the grid's position is set during password creation by placing it such that there is a uniform tolerance area centered around the original click-point, by calculating the appropriate ðx; yÞ grid offset (Gx; Gy) (in pixels) from a(0,0) origin at the top-left corner of the image. On subsequent user login, the system uses the originally recorded offsets to position the grid and determine the acceptability of the each login click-point.

For each password P_W, the system hashes the username W, as a unique salt intended to force user specific attack dictionaries, and the following details for each click-point $C_i$ði¼1 . . .5Þ: its grid offset ðGx$_i$;Gy$_i$Þ, a tolerance area identifier Tx$_i$; Ty$_i$ (indicating the exact square containing the click-point),and its image identifier I_i. The system also stores the following additional information A_W in the clear: Gx; Gy for each click-point and a random seed S_W used to determine the pool of images for a given user (see Section 8.2).These components are described as

C_i¼ðI_i; Tx$_i$; Ty$_i$;Gx$_i$;Gy$_i$Þ

P_W ¼hð½C_1. . .C_i; WÞ

A_W

¼ð½Gx_1;Gy_1...Gx_i;Gy_i
;S_WÞ:

The discretization grids and offsets are transparent and unknown to users. An attacker who gained access to this information would not know the user's password, but might try to use it to guess higher probability click-points, e.g., by overlaying corresponding grids onto images looking for popular target points centered within grid squares. Whether this provides any attack advantage over trying to exploit hotspots without grid information remains an open question.

Deterministic Image Sequencing

Each image is displayed using a deterministic function. During login, the sequence of images is regenerated. This approach allows a different sequence of images per each user while still guaranteeing a consistent mapping of click-points to images for each user. If a password is changed, a new S_W is generated.

Using this implementation, there is a possibility that images are reused for a given user. For example, a user clicking on an incorrect location during login might, by chance, see an image belonging somewhere else within their password. While this poses a potential usability concern, the likelihood of this happening is correspondingly low with enough images. There is no evidence this occurred in any of our studies. The image selection algorithm could be modified to disallow all image reuse for a given user, albeit possibly providing enough verifiable information to determine the entire password to an attacker who learns only the last image: if each possible traversal of images is unique, knowing the last image means that with effort, an attacker could find the unique password that ends with that particular image. This avoids the situation where multiple locations lead to the same next image, breaking the implicit feedback property of PCCP and likely confusing users. All images could be reused at each stage in the password and for every user. This strategy has the highest probability of collision where a user clicks on incorrect click-point and unfortunately sees an image belonging else wherein their password. This probability can be reduced or nearly eliminated if the overlap of images is reduced between password stages, increasing the number of images in a user's set.

An alternative to increasing the number of images is to use larger images but crop them differently for each user. Hotspot analysis would be more difficult for attackers because the coordinates of hotspots could not be directly applied across accounts. If furthermore, each user receives a different pool of images (perhaps as an overlapping subset of the overall set of images in the system, as determined by S_W and f),an attacker would need to collect these data on a per-user basis when launching an attack.

Viewport Details

The viewport visible during password creation must be large enough to allow some degree of user choice, but small enough to have its intended effect of distributing click- points across the image. Physiologically, the human eye can observe only a small part of an image at a time. Selecting a click-point requires high acuity vision using the fovea, the area of the retina with a high density of photo receptor cells. The size of the fovea limits foveal vision to an angle of approximately 1 degree within the direct line to the target of interest. We chose the size of the viewport to fall within this area of sharp vision.

5.CONCLUSION

A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred(at some cost in usability)from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The approaches discussed in this paper present a middle ground between in secure but memorable user-chosen passwords and secure system- generated random passwords that are difficult to remember.

The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users actions. In PCCP, creating a less guessable password(by selecting a click point within the first few system-suggested viewport positions)is the easiest course of action. Users still make a choice but are constrained in their selection.

References

1. S. Chiasson, R. Biddle, and P. vanOorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS),July 2007.

2. S. Chiasson, A. Forget, R. Biddle, and P. vanOorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture,Creativity, Interaction,Sept.2008.

3. S. Chiasson, A. Forget, E. Stobert, P. vanOorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

4. E. Stobert, A. Forget, S. Chiasson, P. vanOorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf.(ACSAC),2010.

5. S. Chiasson, A. Forget, R. Biddle, and P. C. vanOorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'lJ. Information Security, vol.8, no.6, pp. 387-398, 2009.

6. J. Yan, A. Blackwell, R. Anderson, and A.Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranorand S.Garfinkel,eds.,ch.7,pp. 129-142,O'ReillyMedia, 2005.

7. S. Chiasson, P. vanOorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS),pp. 359-374,Sept.2007.

8. L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.

9. L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91,no. 12,pp. 2019-2020, Dec.2003.