Graphical Password Authentication using Persuasive Cued Click-Points Mechanism

V. Prasath, R. Buvanesvari, P. Nithin, S. Banu, K. Rajeswari

Abstract- This 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.

Keywords- Persuasive Cued Click-Points

I. 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. Textual passwords can be replaced by the recent strong secure and reliable method, Graphical based password [3]. A password authentication system should encourage strong passwords while maintaining memorability. 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 [4]. 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.

Researchers are developing various graphical alternatives to the traditional text password. For example, Real User employs facial photographs in its graphical-password system. The system picks five faces at random from a database and users log on by selecting those five from a grid containing other, decoy faces, explained Paul Barrett, Real User's chief executive officer. Users remember faces more easily than other types of graphical elements, according to Barrett, and this ability is not linked to factors such as age, education, or intelligence. Graphical passwords were first proposed by Blonder.

Manuscript received January 15, 2014.

V.Prasath, Assistant Professor, Department of Computer Science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India.

R.Buvanesvari, Assistant Professor, Department of Computer Science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India.

P.Nithin, Final Year UG Student, Department of Computer science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India.

S.Banu, Final Year UG Student, Department of Computer science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India.

K.Rajeswari, Final Year UG Student, Department of Computer science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India.

In his scheme, a password uses an image in which many small regions have been delineated. The user has to choose some of these regions as a password and in order to log in later; the user must click in each of the chosen regions (with a mouse or a stylus).The user must remember the chosen click regions and keep them secret [5].

On the other hand, allowing arbitrary click points leads to a robustness problem: Usually a person will not be able to click repeatedly on exactly the same places, which means that the password clicked on by the user is "a little" different from the password that was originally chosen. Allowing approximately correct passwords, however, prevents the use of cryptographic password hashing (also known as "password Encryption") since passwords that are approximately (but not exactly) the same will usually have very different hash values. Cryptographic password hashing is important because it enables secure storage of passwords in an insecure storage environment [6].

II. BACKGROUNDS

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.

2.1 Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall [7]. Example systems include Pass Points and Cued Click- Points (CCP).

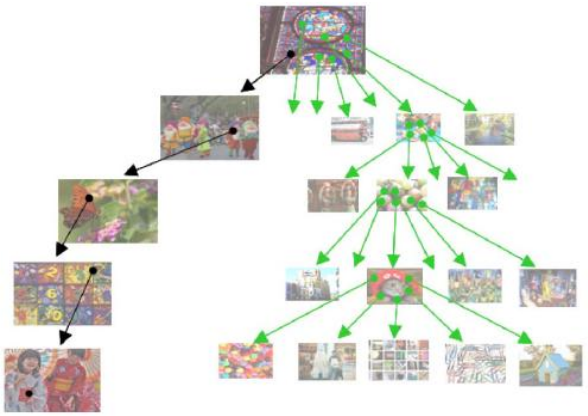

Fig 1: A user navigates through images to form a CCP password. Each click determines the next image.

Fig 2:Pool image (unmodified version from) with the first seven steps in the scan-path.

2.2 Persuasive Technology

Persuasive Technology was first articulated by Foggas 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 [8]. 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).

III. PERSUASIVE CLICK POINTS

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. 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 [9]. Specifically, when users create a password, the images are slightly shaded except for a viewport (see Fig. 3). 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 variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this highlighted 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. Our system supports users in selecting passwords of higher security .Persuasion helps to influence user's choice in click-based graphical passwords by encouraging them to select more random click-points[2].

During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

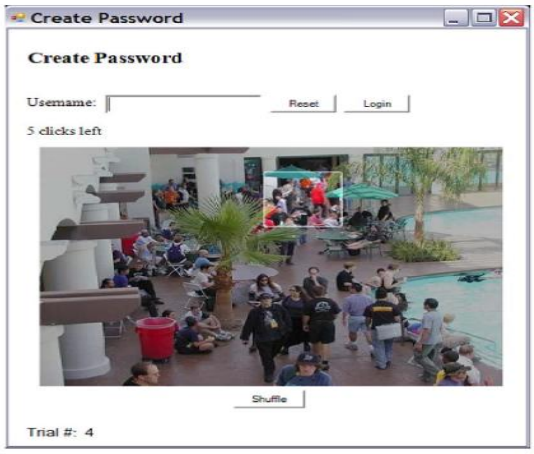

Fig 3: PCCP Create Password interface. The viewport highlights part of the image.

The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password.

IV. ANALYSIS OF PASSWORD DISTRIBUTIONS

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 spat stat, a spatial statistics package for the R programming language. The J-statistic from spatial analysis was used to measure clustering of click-points within data sets (the formation of hotspots)[10]. The J-statistic combines nearest neighbor calculations and empty-space measures for a given radius r to measure the clustering of points. A result of J closer to 0 indicates that all of the data points cluster at the exact same coordinates, J = 1 indicates that the data set is randomly dispersed, and J > 1 shows that the points are increasingly regularly distributed. For passwords, results closer to J(r) = 1 are desirable since this would be least predictable by attackers. We examined clustering at J (9) for the set of core images common across studies with at least 30 click-points per image for each study. A radius of nine pixels approximates the 19 X 19 tolerance squares used by the system during password reentry.

To compare sets of J-statistics to each other, we employed the following technique. Regarding the data as categorical, six categories stemming from the possible orderings are identified: (PCCP-CCP-PP), (PCCP-PP-CCP), (PP-CCPPCCP), (PP-PCCP-CCP), (CCP-PP-PCCP), and (CCP-PCCPPP). Fig.4 shows the ordering for each of the 17 images. For example, the bee image falls in the PCCP-CCP-PP category because J (9) for PCCP exceeds J (9) for CCP, which exceeds J (9) for Pass Points.

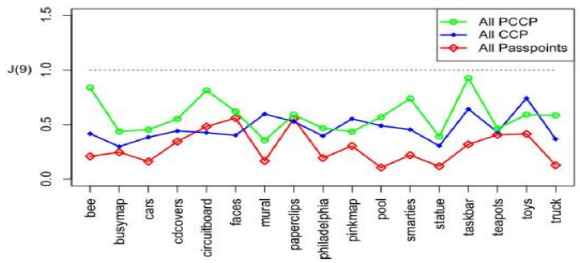

Fig 4: J(9) for the 17 core images, for all studies.

V. SECURITY

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

5.1 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 of 243, success after 242 guesses). However, skewed password distributions could allow attackers to improve on this attack model. Section 6 examined the password distributions based on several characteristics. We now consider how these could be leveraged in guessing attacks.

5.1.1 Pattern-Based Attack

One of the proposed attacks on Pass Points 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 [11]. The attack guesses approximately half of passwords collected in a field study on the Cars and Pool images (two of the 17 core images) with a dictionary containing 235 entries, relative to a theoretical space of 243. Given that PCCP passwords are essentially indistinguishable from random for click-point distributions along the x- and y-axes, angles, slopes, and shapes, such pattern-based attacks would be ineffective against PCCP passwords.

5.1.2 Hotspot Attack with All Server-Side Information

Pass Points passwords from a small number of users can be used to determine likely hotspots on an image, which can then be used to form an attack dictionary. Up to 36 percent of passwords on the Pool image were correctly guessed with a dictionary of 231 entries. The attacker's task is more difficult for PCCP because not only is the popularity of hotspots reduced, but the sequence of images must be determined [1]. And also each relevant image is collected, making a customized attack per user. An online attack could be thwarted by limiting the number of incorrect guesses per account [12].

5.2.2 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.

5.2.3 Social Engineering

For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail. One preliminary study suggests that password sharing through verbal description may be possible for Pass Points. 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 [13].

VI. CONCLUDING REMARKS

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 insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember.
Finally, our attacks could be used to help inform more secure design choices in implementing Pass Points-style graphical passwords. Proactive checking rules for Pass Points-style graphical passwords might be created based on the click-order pattern attacks herein, for example, disallowing LINE or DIAG patterns (for all laziness modes), and disallowing passwords where too few click-points are further than 150 pixels away from the previous click-point. Of course, any such proactive checking rules would need to be tested to ensure that the usability impact is acceptable and that security is not impacted in other unexpected ways.

REFERENCES

1. Tara H R, Usha and Ganeshayya I Shidaganti, "Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points", June – 2013
2. Sonia Chiasson ,Elizabeth Stobert, Alain Forget, Robert Biddle and Paul C. Van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", March 2012
3. Wazir Za ada Khan, M Y Aalsalem and Yang Xiang, "A Graphical Password Based System for Small Mobile Devices", September 2011.
4. S.Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
5. S.Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
6. S.Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.
7. 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.
8. 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. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
9. L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
10. D. Florencio and C. Herley, "A Large-Scale Study of WWWPassword Habits," Proc. 16th ACM Int'l World Wide Web Conf.(WWW), May 2007.
11. M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), 2010.
12. D. Florencio and C. Herley, "Where Do Security Policies Come from" Proc. Symp. Usable Privacy and Security, 2010.