Authentication Features Based on Sound Signatures

[1]Medisetty baby Anusha, [2]P.Radha Krishna
[1]Final M Tech Student, [2]Head of the Dept
[1,2]Dept of Computer Science and Engineering, Nova college of Engineering & Technology, Jupudi, Ibrahimpatnm, Vijayawada

Abstract: Providing user security in image processing is the main contribution in present days. Due to this traditionally developed application is Persuasive Cued Click Points graphical password schema. An important usability goal for knowledge based authentication system is to support evaluations, and implementation considerations. Traditionally we develop persuasion to influence user choice in click based graphical passwords encouraging users to select more random, and hence more difficult to guess, click points presentation process. We propose to extend our existing work for supporting sound signature processes for higher authentications in integrating security of data for accessing services. Our experimental results show efficient data security in login process authenticated by the other users.

Index Terms: Usable security, Authentication, graphical passwords, Sound Signature.

I. INTRODUCTION

User authentication is a main component of almost all security applications. The weaknesses of using text based passwords for authentication are well known and there is a significant body of recent research exploring the feasibility of graphical approaches to provide a more secure and usable alternative. Based on the studies showing that human brain is best at recalling images than text, graphical positive identifications are to resolve memory burden and little password area problem of classical passwords. Another solution to generate strong passwords is password managers. These manager programs can be implemented as plug-ins to web browsers and they translate easy to remember and low-entropy passwords into stronger passwords, which are immune to dictionary, attacks. For maintaining the memorability, the password authentication system should encourage strong passwords. We propose that authentication schemes which, allows the user choice to influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to Predict) is more tedious, prostate users from making such choices. Moreover, in the effect of this approach makes choosing a more secure password the path-of- least-resistance. It is easier to follow the system's suggestions for a secure password a feature lacking in most schemes rather than increasing the burden on users. Using above process in graphical password interaction we will introduce the first Persuasive Cued Click Points and conducted user studies evaluating usability and security. This analytical examination provides a comprehensive and integrated evaluation of PCCP covering each usability and security issues, to prior understanding as is prudent before practical readying of new security mechanisms. Through eight user studies. In this paper we are introduce the specialized technique for protecting user data. By controlling the pattern design in data representation using hotspots for increasing the usability in data retrieval. In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

II. RELATED WORK

Text passwords are the most popular user authentication method even though it has security and usability problems. Preference such as biometric systems and tokens has their own drawbacks. The extension implemented is user-friendly and provides a more secure user experience. Consider for an instance in our system it is obvious when the plug-in has been activated and is awaiting input and thus the solution alleviates the problems associated with incorrectly assumed state of the system. With any authentication, system there is a risk of memory interference, where users are expected to recall information to log in. Multiple password interference occurs when users must remember passwords for many systems and the memories of the different passwords interfere with each other. Studies have shown that users typically create easy-to-guess text passwords and reuse these passwords across several accounts.

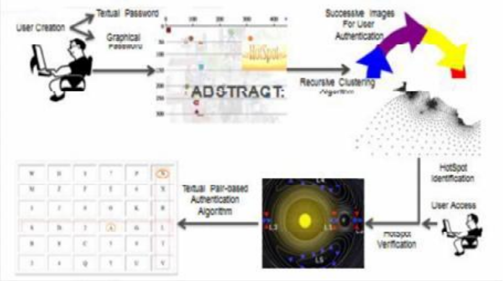


Figure 1: Hotspot verification in authentication system.

We are interested in the graphical password approach. It has been suggested that graphical passwords may be less susceptible to multiple password interference since humans have better memory for recognizing and recalling images than text.

Cued-recall: Users identify and target previously selected locations within one or more images. PCCP is stronger against password-guessing attacks than other click-based password systems and maintains login times and success rates comparable to text passwords.

Persuasive Technology: Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology should guide and encourage users to select stronger passwords i.e. an authentication system, but not impose system- generated passwords. To adequate, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As mentioned, the 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.

III. EXISTING APPROACH

Persuasive Cued Click-Points (PCCP): We investigated whether the system could influence users to select more random click-points while maintaining usability The goal was to encourage more secure behavior by making less secure choices (i.e., choosing poor or weak passwords) more time consuming and awkward. In effect, behaving firmly became the safe path-of-least-resistance. The viewport is positioned indiscriminately, instead of specifically to avoid far-famed hotspots, since such info may allow attackers to improve guesses and could cause the formation of recent hotspots. We evaluated the usability of PCCP through several performance measures. We compared PCCP, the results in context, to the other authentication schemes tested under similar conditions. Statistical analysis was used to determine whether differences in the data reflected actual differences between conditions or might reasonably have occurred by chance.

IV. PROPOSED APPROACH

A password authentication system should encourage strong passwords while maintaining memorability. The proposed authentication schemes allow user choice while influencing users toward stronger passwords. Our scenario says the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, prostate users from making such choices. Moreover, in the effect of this approach makes choosing a more secure password the path-of-least-resistance. It is easier to follow the system's suggestions for a secure password a feature lacking in most schemes rather than increasing the burden on users. 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. The PCCP approach is to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP).

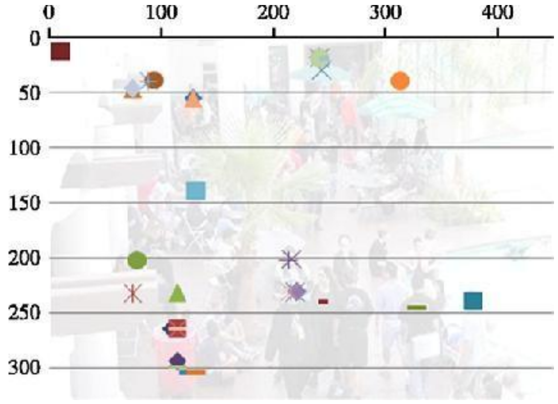


Figure 2: Points object detection in cued clicks.

As shown in figure we are finding out the efficient image interaction based on the features present in the image. Decreasing the pattern difference in each image based on hotspots invariance.

Shuffles:

During password creation, PCCP users may press the shuffle button to randomly reposition the viewport. For click-points across users, fewer shuffles lead to more randomization. The shuffle button was used moderately. Consider the example since PCCP Lab passwords involved five images and the mean number of shuffles per password would be 3 < 5 =

15. PCCP Lab study users who shuffled a lot had higher login success rates than those who shuffled little and the result was statistically significant.

Varying System Parameters: Mean times for each condition are generally elevated compared to times in the studies with smaller theoretical password spaces. In time taken, to create a password, there is no clear pattern emerges. A general increase in times can be seen in both the login and recall phases as more click points or larger images are used. The participants took much longer to reenter their passwords after two weeks (recall) as expected, reflecting the difficulty of the task.

Usability Results: Overall, PCCP has similar success rates to the other authentication schemes evaluated (CCP, Pass Points, and text). PCCP password entry takes a similar time to the other schemes in the initial lab sessions. The results indicate longer recall times for PCCP when recalling passwords beyond the initial session. The more shuffled users had significantly higher success rates in the PCCP Lab study. However the difference in success rates between high and low shufflers was not statistically significant for the two-week or web studies. In additional, users reported favorable opinions of PCCP in post-task questionnaires.

Pattern-based attack: 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.

Sound Signature Patterns: We have integrated sound signature to help with the password. No system has been devolved so far which uses sound signature and graphical password authentication. Study says that sound signature or tone can be used to add facts like images, text etc. Our idea is inspired by this novel human ability. Research says that human can remember images as well as sound tone easily; by applying this method we design our project so it will provide more security. Observed that all student who were registered entered their graphical password and video sound clip and it will be more secured from their point of view it is very good for Graphical and sound clip password authentication system.

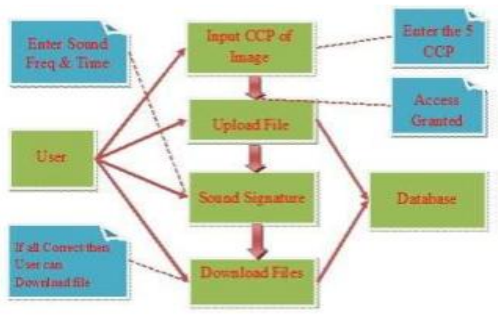
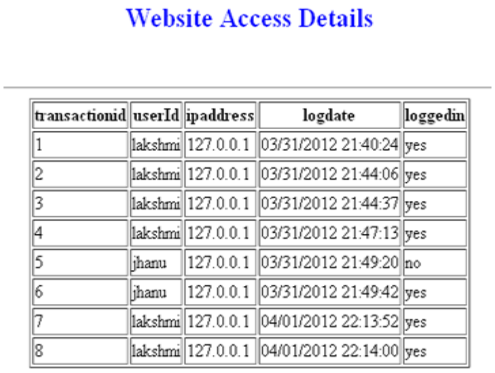


Figure 3: System Architecture

Firstly we need to enter the CCP of image. If entered CCP's are correct then system will allows user for next level of logging. In next level user required to enter the volume level, if volume level is correct system will allows for next authentication level. In last stage of logging user need to enter correct video timing. If any of them (CCP's, Volume level, Video timing) are incorrect then system will go in halt state for next 12 hours. After completion of 12 hours reboot again and user can try for uploading and downloading of data by entering correct password for all stages.

V. EMPIRICAL RESULTS

In this section we describe the comparative results between persuasive cued click point interactions in each image. We are designing the user interface for accessing an account. In that, every user interacts with username and password description, for as normal user login in various applications. Only difference is that, in this requirement we are introducing the graphical passwords instead of text passwords. In text passwords security considerations are less because every known user can access previous user login details. However, in graphical password we are introducing pattern image with hotspots based on the user known history. User history can be stored in image features of presented image formulation.



Website Access Details

transactionid	userId	ipaddress	logdate	loggedin
1	lakshmi	127.0.0.1	03/31/2012 21:40:24	yes
2	lakshmi	127.0.0.1	03/31/2012 21:44:06	yes
3	lakshmi	127.0.0.1	03/31/2012 21:44:37	yes
4	lakshmi	127.0.0.1	03/31/2012 21:47:13	yes
5	jhanu	127.0.0.1	03/31/2012 21:49:20	no
6	jhanu	127.0.0.1	03/31/2012 21:49:42	yes
7	lakshmi	127.0.0.1	04/01/2012 22:13:52	yes
8	lakshmi	127.0.0.1	04/01/2012 22:14:00	yes

Figure 4: Website accessing design stored details.

As shown in above Firstly we will find the position of the each image present in the graphical password interaction.

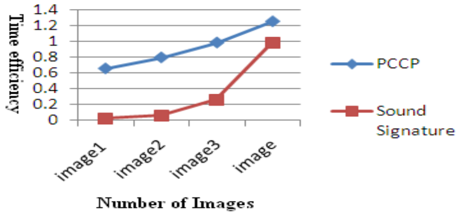


Figure 5: Comparison results with accessory

For PCCP, half of click-points fall within the within the top 14.6% hotspots on the worst-case image. This analysis focused on individual click-points and not entire passwords. Nevertheless, the recommended implementation the attackers get no partial feedback on correctness partway through an offline guess, precluding divide-and-conquer (piecewise) attacks on PCCP.

VI. CONCLUSION

Better user interface design can influence users to select stronger passwords. The main objective in PCCP is that creating a harder to guess password is the path-of-least-resistance likely to make it more effective than schemes where secure behavior adds an extra burden on users. The schema has proven effective at reducing the formation of hotspots and patterns and increasing the effective password space. In our approach makes choosing a more and secure password the path of least resistance. Moreover increase in the burden on users and it is getting easier to follow the system's suggestions for a secure password.

VII.REFERENCES

1) Emerald Assessing Image Based Authentication Techniques In A Web (www.Emraldinsight.Com).

2) Sonia Chiasson, Member, IEEE journal, Alain Forget, Elizabeth Stobert, Robert Biddle, Member, IEEE, And P. C. Van Oorschot, Member in IEEE journal, "Persuasive Cued Click-Points: Design, Implementation, And Evaluation Of A Knowledge-Based Authentication Mechanism", Edition: Oct, 2011.

3) Kemal Bicakci, Mustafa Yuceel, Burak Erdeniz," Graphical Passwords As Browser Extension: Implementation And Usability Study", By K Bicakci- 2009.

4) Sonia Chiasson, Alain Forget, Elizabeth Stobert "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords", the definitive version was published in ACM CCS'09 November 9–13, 2009.

5) Elizabeth Stobert, Alain Forget, Sonia Chiasson, "Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords", ACSAC '10 Dec. 6-10, 2010, Texas, USA.

6) S.Wiedenbeck, J.Waters, J. 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. 1-2, pp. 102–127, 2005.

7) "Authentication using graphical passwords: Effects of tolerance and image choice," in 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.

8) K. Golofit, "Click passwords under investigation," in 12th European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007.

9) A. Dirik, N. Menon, and J. Birget, "Modeling user choice in the Passpoints graphical password scheme," in 3rd ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

10) J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in 16th USENIX Security Symposium, August 2007.

11) A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On purely automated attacks and click-based graphical passwords," in Annual Computer Security Applications Conf. (ACSAC), 2008.

12) P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on PassPoints-Style graphical passwords," IEEE Trans. Info. Forensics and Security, vol. 5, no. 3, pp. 393– 405, 2010.