International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3, March 2016
ISSN: 2395-3470
www.ijseas.com

UNPREDICTABLE PASSWORD GENERATION USING GRAPHICAL AUTHENTICATION AND DECENTRALIZED ENCRYPTION

G.Kalpana[#1], G.Akshaya*[2].

[#]Dept. of Computer Science and Engineering SRM UNIVERSITY, Ramapuram,
Chennai, Tamilnadu, India.
* Dept. of Computer Science and Engineering, SRM UNIVERSITY, Ramapuram
Chennai, Tamilnadu, India,

Abstract—**Privacy is which data can be safely disclosed without leaking sensitive information. The objective of a knowledge based secure system is to select stronger passwords for the users and to provide them secret keys. In this paper, a multi-authority decentralized encryption scheme is proposed which provides secret keys without knowing the global identifier of the user. This scheme issues secret keys without any cooperation from the different authorities. Any authority is free to join or leave the system. Users can select passwords of higher strength using click-points. Persuasive technology is used for generating graphical passwords.**
Keywords-***Graphical passwords,privacy,decentralized encryption,secure system.***

I. INTRODUCTION

Security is the avoidance of, or protection against, access to data by unauthorized recipients, and intentional but unauthorized destruction or modification of that data. Computer security is commonly associated with three core areas, which can be suitably summarized by the acronym "CIA": Confidentiality -- Ensuring that data is not accessed by unauthorized persons. Integrity -- Ensuring that data is not modified by unauthorized persons in a way that is not measurable by authoritative users**.** Authentication -- Ensuring that users are the persons they claim to be. Computer security is not restricted to these three broad concepts. Additional ideas that are often considered part of the taxonomy of information security include access control, no repudiation, availability, privacy. Privacy is ensuring that persons maintain the right to control what data is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for. In this paper, a knowledge based authentication scheme is proposed to support users in selecting random and secure passwords. The problems of knowledge-based authentication, typically text-based passwords are well known. Users often create unforgettable passwords that are easy for attackers to guess, but strong system-assigned passwords are hard for users to memorize. So people select expected passwords. Users tend to choose

passwords that are memorable in some way, which unfortunately often means that the passwords tend to follow expected patterns that are easier for attackers to exploit. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. An authentication system should encourage strong passwords while still maintaining memorability. In this paper, a multi-authority encryption scheme is proposed to issue secret keys to the users independently without any cooperation from the authorities.

II. PROBLEM STATEMENT AND SOLUTION

A. *Problem Definition*

The focus here is to provide privacy by issuing secret keys and to support users in generating secure passwords maintaining authentication.

B. *Proposed Solution*

A knowledge based password authentication should itself suggest passwords rather than forcing the users to create them. It should encourage strong passwords while maintaining memorability. Users often find difficult to remember stronger passwords and create text based memorable passwords which are easy for the attackers to guess. The problem is that the users again find difficult to remember system assigned text passwords. For this, click-based graphical passwords are used where users identify and target a click point on an image is according to which a password is generated. Persuasive Cued click Points (PCCP) encourages users to select less

predictable passwords and makes it more difficult to select passwords where all five click-points are hotspots.

C. *Related Work*

Cued Click Points (CCP) is a technique where the images act as memory cues to help in recall. Hotspots are the areas of the images that have higher likelihood of being selected by the users as password click points. Users tend to select their click points on predictable patterns like straight lines which becomes easy for the attackers to gain knowledge about the passwords. CCP [5] uses one click-point on five different images instead of five click-points on a single image. The next image is displayed based on click point chosen by the user. Users select their images only to the extent that their click point determines the next image. Password entry becomes easier where each image triggers the memory of a corresponding click point. The order of images need not be considered by the users as the system represents only one image at a time.

III. SYSTEM METHODOLOGY

A. *Creating secure passwords using PCCP*

This section describes an authentication system that applies persuasive feature to CCP to overcome the demerits of CCP. According to the previous section, the hotspots and patterns reduce the security of click-based graphical passwords as attackers can predict those from the patterns. This suggests that if users select their own click –points without guidance, hotspots will remain an issue. PCCP [3] displays the images as slightly shaded except for a viewport while the users create passwords. The viewport is positioned randomly to avoid known hotspots. Users must select a click-point within this highlighted viewport and cannot click outside unless they press the shuffle button. This button randomly repositions the viewport. The viewport and shuffle button appears only during password creation. The images will be normally displayed while users enter their passwords allowing users to click anywhere on the images. The theoretical password space for a password system is the total number of unique passwords that could be generated. A larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. Text passwords have very skewed distributions resulting in an effective password space much smaller than the theoretical space but PCCP is specifically designed to reduce such skews.

1) *Performance Measures*

The viewport is a tool to help users to select more secure passwords and they could shuffle as many times as they wish to find a suitable click-point. Here, minimum six click-points are used to create a stronger passwords. 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 user presses the login button but the password is incorrect. Restarts occur when the user presses the reset button midway through password entry and restarts password entry. Times are reported in seconds for successful password entry on the first attempt. The entry time which is the actual time taken from the first click-point to the sixth click-point.

2) *Password Distributions and Hotspots*

Users are provided with the shuffling strategy. They either shuffle a lot or barely shuffle to select secure click-point. Those who barely shuffle select their click-point by focusing on the section of the image displayed in the viewport and those who shuffle a lot scan the entire image and select their click-point and proceed to shuffle until the viewport reach that area. Users who barely shuffle feel that the viewport make it easier to select a secure click-point. Those who shuffle a lot feel that the viewport hinder their ability to select the most obvious click-point on an image and that they have to shuffle repeatedly in order to reach the desired point. The J-statistic from spatial analysis is used to measure clustering of click-points within datasets. 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 the data point 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 for the attackers.

PCCP's shuffle mechanism and viewport are more effective in reducing clustering when used with larger images. This is due to the proportionally smaller area covered by the viewport in relation to the total size

of the image making it less likely that known hotspots are available for selection. PCCP click points have a flatter distribution and thus an attack dictionary based on hotspots should be less effective for PCCP than for the other schemes. This analysis focus on individual click-points and not entire passwords. Attackers get no partial feedback on correctness partway through an offline guess, precluding divide-and-conquer attacks on PCCP. With one image, as in PassPoints, users tend to start at one corner of the image and progress across the image with each subsequent click-point. However, with PCCP, users see a new image for each click-point and tend to select each click-point independently, with no regard to its ordinal position within the password. With respect to angles and slopes formed between adjacent line segments within passwords, analysis shows that PCCP passwords have large angles and favor no particular location. Similarly, the frequency distributions for the overall shapes formed by following the path from the first to last click-point for PCCP are within the range of the random data sets. It is unlikely that users chose passwords consisting of very similar colors. Visual inspection of the passwords revealed no other evident relationships

B. *Multiple-authority attribute-based encryption*

In this scheme, multiple authorities can work independently without any cooperation. The GID [2] is used to tie all the user's secret keys together, while the corrupted authorities cannot pool the user's attributes by tracing it. This method is based on standard complexity assumption. Here, user executes a 2-party secure computation protocol with an authority to obtain his secret keys. As a result, the user can obtain his secret keys anonymously without releasing anything about his identifier to the multiple authorities. As pointed in [4], an anonymous credential system [6] can be used by the user to convince the authorities that he holds the corresponding attributes without revealing his identifier. In an anonymous credential system, a user can obtain a credential and prove the possession anonymously. The user can interact with different partners with different pseudonyms such that no partner can link the pseudonyms to the same user. Furthermore, the user can prove that he has obtained multiple credentials which correspond to the same identifier without revealing it. Hence, this technique can be employed in our system to allow the user to obtain the corresponding secret keys without revealing his identifier to the authorities. To be secure against the collusion attacks, the user's identifier is embedded in his secret keys and bound with the second secret keys of the authorities so that these keys can be tied together. When encrypting a message, all the second public keys of the authorities are aggregated. Therefore, only the secret keys from the same identifier can be used to decrypt the ciphertext.

C. *Evaluation Metric*

The following are the results in implementing the multi authority attribute based encryption and PCCP.

1. PCCP has the least clustering of click-points across different users.
2. According to hotspots analysis, PCCP has the flattest click-point distribution and is least likely to contain hotspots when compared to CCP.
3. Color analysis shows that users do not choose click-points within passwords based on color.
4. The attribute based encryption can be used as a sound solution to construct privacy-preserving data transfer and access control schemes.
5. Users can obtain secret keys from multiple parties without being traced and exposing their identities to the authorities

IV. CONCLUSION

The objective of a password authentication system is to maximize the effective password space. This impacts usability when choice is involved. Tools such as PCCP's viewport cannot be exploited during an attack. The approaches discussed in this paper present a secure system-generated random passwords that are difficult to remember. Providing information on creating secure passwords using password managers or providing tools such as strength meters for passwords have had only limited success [1]. 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 user's actions. In PCCP, creating a less guessable password click-point within the first few system-suggested viewport is the easiest course of action. Better user interface design can influence users to select stronger passwords. A key feature in PCCP is that creating a harder to guess password is the path of least resistance, making to more effective than schemes where secure behavior adds an extra burden on users. The approach has proven effective at reducing the formation

of hotspots and patterns, thus increasing the effective password space. In the decentralized encryption, all the user's keys are tied to his identifier to resist the collusion attacks while the multiple authorities cannot know anything about the user's identifier. Notably, each authority can join or leave the system freely without the need of reinitializing the system and there is no central authority. Any access structure can be represented using the access tree technique.

REFERENCES

[1] D. Florencio and C. Herley, "A Large-Scale Study of WWW Password Habits", Proc. 16th ACM Int'l World Wide Web Conf. (WWW), May 2007.

[2] Jinguang Han, Willy Susilo, Yi Mu and Jun Yan, "Privacy-Preseving Decentralised Key-Policy Atrribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems.

[3] 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", IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, March/April 2012.

[4] M. Chase and S. S. Chow , " Improving privacy and security in multi-authority attribute-based encryption", in Proceedings: ACM conference on Computer and Communications Security- CSS'09(E. Al-Shaer, S. Jha and A. D. Keromytis, eds.), (Chicago, Illinois, USA), pp. 121-130, ACM , November 9-13, 2009.

[5] S.Chiasson, P. van Oorschot and R. Biddle , "Graphical Password Authentication using Cued Click Points", Proc. European Symp. Research in Computer Security(ESORICS), pp. 359-374, Sept. 2007.

[6] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation", in Proceedings: Advances in Cryptology- EUROCRYPT'01 (B. Pfitzmann, ed.), vol. 2045 of Lecture Notes in Computet Science,(Innsbruck, Ausria), pp.93-118, May 6-10, 2001

.