IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

Knowledge-based authentication: investigating the use of persuasive cued click points

MS.J.SWATHI[1], MS.G.LAKSHMI[2], SD.MEER SUBAN ALI[3]

Abstract

Most users use simple passwords that are easy for hackers to deduce, while robust passwords generated by the system are difficult for end users to remember. This research examines the three-pronged usability and security assessment of the Persuasive Cued Click Points graphical password system. Helping users make informed decisions is a crucial part of any authentication system. Stronger passwords. Improving safety by allowing for more effective password space to be used. Bad passwords contribute to the development of hotspots in click-based graphical passwords, which are regions of an image where users are more likely to choose click-points, facilitating more effective dictionary attacks by hackers. In order to make click-based graphical passwords more secure and harder to crack, the authors of this research used a persuasive technique based on the principle of social influence.

1. Introduction

Users have trouble remembering complicated passwords, and even the ones they can remember are easy to guess [1, 2, 3]. The authentication system should ensure that passwords are difficult to guess while yet being simple to remember. Peace of mind, security, and stability. Users are allowed some leeway in coming up with their own passwords, but are gently guided toward more safe choices. Because it takes more effort, users shouldn't use weak passwords (ones that would be easy for hackers to guess). These authentication mechanisms are inherently clumsy, making it difficult to choose a secure password. Password strength should be suggested by the system, making it easier for users to adopt that password rather than generate one on their own (a feature lacking in most systems).

To create the compelling click-based graphical password system, the technique depends on lab research (including 20 people). Users are more prone to choose click points from certain parts of an image (called "hotspots"), and our research shows that our Persuasive Cued Click Points approach may effectively reduce this number without sacrificing usability. The relationship between tolerance value and security rate is analyzed in this paper. Many people argue that visual passwords are the best form of authentication since it's straightforward to compare the password preferences of various users. The method's flexibility to text-based passwords is highlighted.

2: Context

Despite their popularity, text passwords pose usability and security issues. There are other options, such as biometric systems and tokens, but they also have their drawbacks. [1]- [3]. The primary emphasis of this effort will be on a Passwords consisting of pictures are an alternate method. Blonder developed graphical passwords in 1996 [3]. Visual password generators may be broadly categorized into recognition-based and recall-based approaches. Users who choose to use a recognition-based authentication method may verify their identities by reviewing a set of photos and selecting the same images they selected during the registration process. The user will be asked to remember a graphical password they created or choose during registration. The basis of this work is the method of recalling past experiences. Knowledge-based authentication systems often run into problems due to the prevalence of text-based passwords. Strong system-assigned passwords are famously difficult to remember, whereas weak user-created passwords are notoriously easy for hackers to break. Users are encouraged to choose strong passwords that are nevertheless simple enough to remember when a password authentication mechanism is in place.

ASSOCIATE PROFESSOR[1,2,3]
COMPUTER SCIENCE ENGINEERING
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY
(jillaswathi@gmail.com),(lakshmiraj2006feb@gmail.com), (meersubanali@gmail.com)

International Journal of Information Technology & Computer Engineering
ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

It is proposed that authentication techniques provide users the option of using a strong password. The system discourages the use of weak passwords by making it more inconvenient to do so. The hardest part of choosing a stronger password is now overcome by using this technique. With this technique, users don't have to put in extra effort to choose a safe password; instead, they may just follow the system's suggestions.

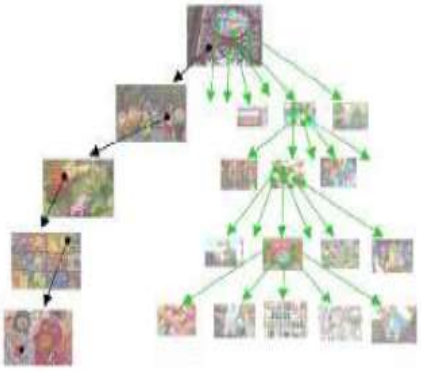

Fig. 1 User navigation trough images to form a PCCP password

The goal of this strategy is to develop a graphical password system with improved usability and security based on user feedback gleaned from usability and security tests conducted on the Persuasive Cued Click-Points (PCCP) prototype. This study offers a unified integration of prior research and two web-based investigations, reinterpreting and updating statistical methodology to account for bigger data sets, and so offering a fresh assessment of passphrase handouts it provides a more thorough security analysis, up to and including the most recent assault on the system, and it lays out key implementation details. In order to improve comprehension before the actual implementation of new security mechanisms, the systematic assessment offers a thorough and integrated evaluation of PCCP including both usability and security problem. PCCP is compared to both text passwords and two comparable graphical password systems via eight user surveys. According to the findings, PCCP successfully eliminates hotspots and prevents patterns from being established by click-points inside a password without compromising usability.

I. Clickable images used as passwords

To take use of people's innate memorization of visual cues, knowledge-based authentication methods like graphical password systems were developed. It has previously been prepared and published where the complete examination of graphic passwords may be found. In this context, it's crucial to have a visually memorable password (also known as the loci metric) that can be accessed with a single click. The user then selects the target from among the designated areas of the image (or images). Images are used here as memory aids by providing visual cues. The Cued Click-Points (CCP) [4] and the Pass Points [5] are two examples of such methods.

A Pass Points password consists of five different areas of an image that may be clicked on (see Fig. 2). Passwords may be established by customers by clicking on various parts of an image. The user must reproduce the exact sequence of clicks made throughout the login process, in the same order in which they were made, within a tolerance square of the original click-points defined by the system. The original authors of these works evaluated the system's efficacy and security. We found that there are certain security vulnerabilities that need fixing, despite the fact that it is usable. "Hotspots," or situations in which users consistently use the same click positions in passwords, are the major source of security issues. If attackers are able to get knowledge about these hotspots, for example by password harvesting or automated image processing, they may be better able to develop attack dictionaries and guess Pass Points passwords. To launch a dictionary attack, an attacker must first compile a list of potential passwords (ideally ordered by decreasing likelihood) and then try each one to see whether it unlocks the target account. An attack might target a single account or extend to multiple others in an attempt to compromise a single one.

Cued Click Points are a feature of PCCP that reduces the visibility of vulnerable areas in an effort to make them less appealing to potential attackers. Instead of five distinct clicking regions on a single picture, CCP presents a sequence of five photographs, each with a single clickable region. Depending on where the user clicks, different parts of an image are shown (see Fig. 3 for an example), customizing the experience for each individual viewer. Picture book Only by moving on from the current image will users be able to access the subsequent images. Because a new visual sequence is produced every time a password is made using different click locations [6].

Because each image can be used to instantaneously recall its related click-points, inputting passwords

International Journal of Information Technology & Computer Engineering
ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

may now be seen as a true cued-remember scenario. Users are relieved of the burden of remembering the sequence in which they clicked on individual photographs since the system presents them consecutively. For trusted users only, the CCP provides access to secret feedback. If a person is trying to log in and an unusual image shows, they will be asked to try again after being advised that their current password was incorrect. After the last click-point, a clear signal of authentication failure is supplied as a defense against incremental guessing assaults. User testing and analysis revealed no evidence of CCP, demonstrating the futility of pattern-based attacks. The results demonstrated that this is still a problem [7], despite the fact that exploiting hotspots involves far more work on the side of attackers.

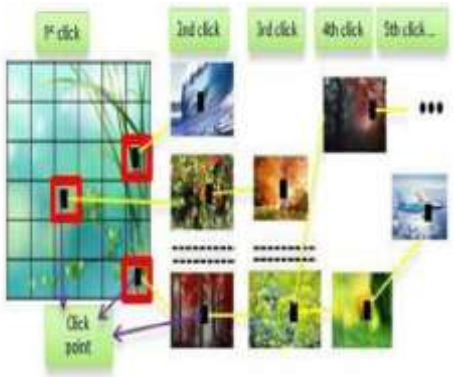

Fig. 2 click points as a password

II. Persuasive Technology

Originally, Fog [8] described persuasive technology as the use of technology to motivate and influence the behavior of people. Persuasion technology in an authentication system should assist and encourage users to choose robust passwords without coercing them to accept passwords generated by the system. The reasons must be taken seriously, and the passphrases that are created must be memorable [9] for this to be of any service. PCCP does this by making it more difficult to choose a weak password. The most difficult thing a user can do is choose a better secure password (one that isn't comprised of known hotspots or predictable patterns). The creation of hotspots among users is mitigated by a more even distribution of click-points. Users are less likely to form hotspots when using this strategy since click points are spread out more uniformly [10, 12].

Hotspots, as shown by previous models, reduce the effective password space and make dictionary assaults more possible, which is a problem with click-based graphical passwords. This research investigated whether encouraging users to choose more randomly dispersed click-points while still achieving the system's minimal criteria may impact their password choices. The major goal was to raise compliance by increasing the difficulty of the less secure behavior (i.e., choosing the weak passwords). Now is the time to choose the difficult route of caution. Using the CCP as a starting point, we implemented a persuasive feature to push users toward more secure passwords and discourage the use of weak passwords that exploit all five of the CCP's weak spot. In this scenario, users created passwords using subtly coloured photos with a randomly located viewport (see Fig. 4). Attackers might utilize this information to improve their guessing and so generate new hotspots, despite the fact that the viewport is placed freely with the exception of avoiding existing hotspots. The viewport's dimensions were optimized to show as many points as possible while still showing an adequate fraction of the whole set. Users were restricted to making clicks inside the highlighted area of the screen. In the event that they don't want to or are unable to choose the click point in the region, they may use the "shuffle" button to cause a random rotation of the viewport. The speed at which new passwords may be generated was drastically reduced since users might rearrange at any time. When I entered my password, a viewport button and a shuffle function appeared. During this last verification step, the viewport did not dim, and the user was free to click wherever on the login page or image.

We hypothesized that a) users might adjust their degree of security to meet their own needs and preferences by considering many viewpoints.

• (b) The user will feel more confident in their decision to enter a potentially hazardous area.

Because users' clicks will be randomly dispersed, no new hotspots will form.

• The success rate of secure logins will increase in comparison to the previous CCP system.

Reducing one's point of view improves login security success rates.

Password sharing will be more comfortable for PCCP users than it was with the CCP.

International Journal of Information Technology & Computer Engineering
ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

Fig. 3 PCCP Create Password interface

For every given password scheme, the theoretical password space is simply the maximum possible number of different passwords. As the theoretical password space grows, the probability that every given guess will be right for a given password decreases. Given an image of dimension ((w h)/t2) c), where w and h are the width and height, respectively, the theoretical password space in PCCP is Click-points in a password are multiplied by the picture's width and height in pixels (w * h) divided by the size of a tolerance square (t2) to yield the total number of tolerance squares per image (c, usually set to 5 in our experiments).

4. SYSTEM DESIGN

Modules for user registration, image selection, and system login make up the system's trifled structure (refer Fig. 5).

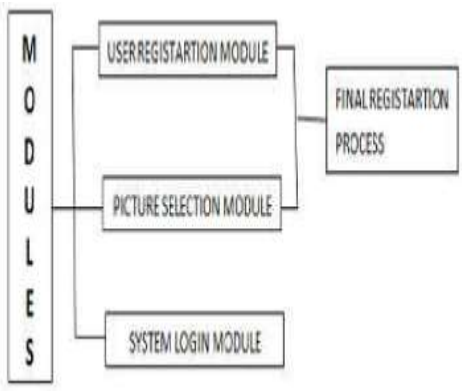

Fig. 4 System modules

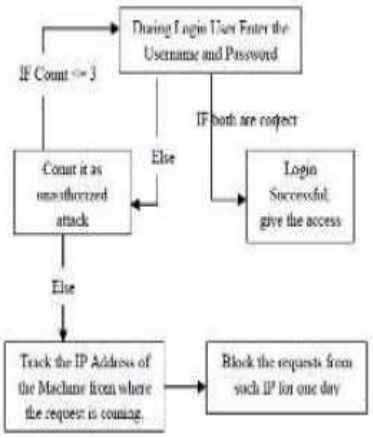

Fig. 5 system login module

In the user registration module, the tolerance value used to compare the registration profile vector with the login profile vector is the user name. Information provided by users during the first registration step is stored in a database and made available during future logins. Here comes the testing and validating part. Users first choose photographs to use as passwords, which are then sliced into a sequence of five clickable spots. Any section of the image may be used as the user's password input. When creating a password, the screen becomes black except from a little view port placed at random. To do any action, the user must first decide where in the window they wish to click. If the user is stuck in the current view port and can't choose a new location, they may just press the Shuffle button to randomly switch to a new one. The view window illustrates that randomly selected passwords are less likely to include hotspots. The user who is determined to click at a certain location may still accomplish it by moving the view port until it reaches the target, but doing so will require much more work and time. After checking in, the photographs display correctly without a viewport, and clicks are repeated in the correct sequence within a tolerance square of the original click-points, as specified by the system.

Diagram of the Process of Adding a New User

Below is a detailed flowchart of the user registration procedure (see Fig. 7), which covers the registration and picture selection phases illustrated in Fig. 6. A user ID and tolerance value are required to begin the procedure. Choosing between one and five click points on the generated photographs is the next step once a user has completed their profile. A user profile vector will be created after the previous actions have been completed.

International Journal of Information Technology & Computer Engineering
ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

Login procedure diagram

In order to access your account, you must first enter your unique user ID that you created upon registration (see Figure 8). The photos are shown correctly, either by shading or the viewport, and they play back the sequence of clicks in the correct order thanks to the system-defined tolerance square of the original click-points. A user's profile vector may be accessed in the manner described above.

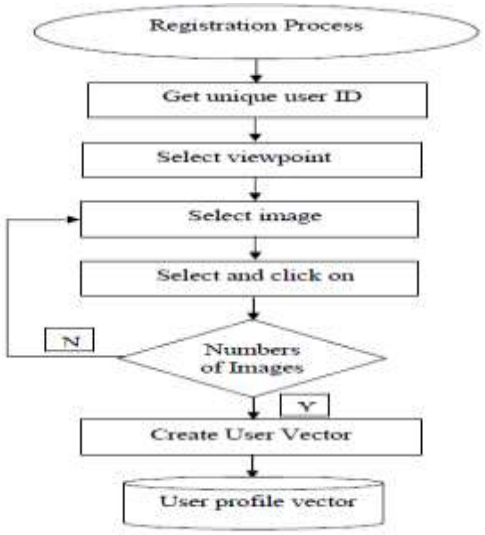

Fig. 6 User registration flowchart

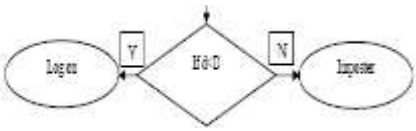

Fig. 7 Login phase flowchart

5. RESULTS

In order to find ways to increase the tolerance value's effectiveness, we conducted a lab study comparing the login success rate and security success rate of existing CCPs with proposed PCCPs.

I. Tolerance value efficiency

Eight participants are chosen at random to begin with. To reveal the secret code, users must choose five clickable areas from among five different photographs. Each image has a large number of unique personalities (image details) that must be clicked on in order to progress. Participants choose a click position in each image in a similar fashion. The participant then uses the password to log in, with the other participants standing in a line behind him and being asked to watch his every move (click points on the images)[14]. When the first user signs out, the other users are asked to enter the same password they just saw.

This value indicates how close you were to the intended "click" position during testing. To account for the fact that users are unlikely to click on an exact pixel, we include a "tolerance zone" that includes the surrounding region. The success rate is the fraction of attempts that are fruitful. Success rates are calculated by summing the runs that completed without any interruptions or restarts. When someone watches you type in a password and reads it over your shoulder, they are "shoulder surfing." In this situation, the assailant is making an effort to kidnap the victim. An attacker is executing a direct password attack if they are able to either intercept user input or deceive victims into exposing their credentials. In table I below, we can see how well the PCCP strategy works in relation to the tolerance value. In Figure 9, we have a graph comparing the success rate in terms of security to the tolerance threshold.

8. CONCLUSION

Authentication systems are designed to help users choose secure passwords and increase the size of the password field. User adoption of strong passwords may be increased by providing a more intuitive interface. Prototyping and usability testing the persuasion method persuasion-cued click-points (PCCP) is a good illustration. From the research we did to ascertain its effectiveness in this setting, we learned that it is both safe and effective. The PCCP guides users in the direction of the safer and more unexpected graphical passwords chosen with a mouse click. PCCP is more effective than systems that make users' adherence to security procedures more of a burden due to its "path-of-high-resistance" approach to password formation. This approach effectively reduces the likelihood of the creation of hotspots, avoids the security flaw known as "shoulder surfing," and provides a high degree of protection without compromising usability.

REFRENCES

A. Singh, and S.B.Sahu This article was first published in the October 2014 issue of the International Journal of Computer Trends and Technology (IJCTT) under the title "Survey on Various Techniques of User Authentication and Graphical Password," which can be found on pages 98-102.

According to [2] "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," by S. Chanson, A. Forget, O. Biddle, and P.C. van

ISN NO: 2347 – 3657
Volume 5, Issue 1, 2019

Borscht (published in IEEE Transactions on Dependable and Secure Computing, Volume 9, Issue 2, Pages 222-235, April 2012).

According to the research of S. Chanson, A. Forget, O. Biddle, and P.C. van Borscht, "Influencing Users Towards Better Passwords: Persuasive Cued Click-Points," was published in the proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, volume 1, September 2008, pages 121-130.

"Secure User Authentication & Graphical Password using Cued Click-Points," by S.B.Sahu and A. Singh, was published in the December 2014 issue of the International Journal of Computer Trends and Technology (IJCTT), volume 18, issue 4, pages 156–160.

According to [5] "Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points," written by Usher T., Tara H. R., and G. I. Shidaganti and published in International Journal of Engineering Research & Technology (IJERT) in June 2013, pp.258-266.

For example: [6] A. Cummings, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," in 2012, available online at http://www.sei.cmu.edu/reports/12sr004.pdf.

According to [7] "Graphical Authentication using Region based Graphical password," published in International Journal of Computer Science and Informatics ISSN, volume 2, issue 3, pages 114-119, February 2012.

[8] "A Novel Gesture Based Graphical Authentication Using Bounding Box and Corner Detection Algorithm," G. Niranjana and K. Dawn, International Journal of Computer Science and Informatics ISSN, vol.12, no.3, pp.114-119, November 2012.

Mood disorders [9] U. D. Yadav, P. S. Publishing "Adding Persuasive features in Graphical Password to increase the capacity of KBAM," in IEEE International Conference on Emerging Trends in Computing, Communication, and Nanotechnology, volume 2, March 2013, pages 513-517.

[10] "Improving Text Passwords through Persuasion," S. Chanson, A. Forget, O. Biddle, P.C. van Borscht, Symposium on Usable Privacy and Security (SOUPS), vol. 4, pp.1-12, July 2008.

According to [11] "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme," by Wei-Chi Ku, Dum-Min Liao, Chia-Ju Chang, and Pei-Jia Qiu, published in Symposium on Privacy and Security in Commutations, volume 4, pages 204-208, October 2014.

Financial Cryptography and Data Security (FC), LNCS, vol.7397, pp.16-24, March 2012; S. Chiasson, C. Decamps, E. Sober, M. Flyway, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, " The MVP Web-Based Authentication Framework,".