AUTHENTICATION FOR ATTACKS IN GRAPHICAL PASSWORDS PASS POINTS STYLE

ASHWINI.J

Department of Computer Science, Pune University
E-mail: ashwini.bedadurge@gmail.com

Abstract— Access to computer systems is often based on the use of alphanumeric passwords. However users have difficulty in remembering passwords that is long and random-appearing. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use. Using graphical passwords users click on images rather than type alphanumeric characters. We have designed a new and more secure graphical password system called passpoints.Based on click-order patterns we introduced a proposed graph-based algorithms to create dictionaries with focus-of-attention scan paths

Keywords- Graphical passwords, Passpoints, Authentication.

I. INTRODUCTION

Graphical passwords have been designed to try to make passwords more memorable and easier to use. Graphical passwords are an alternative to text passwords where user is asked to remember an image or parts of an image instead of a word.We are further discussing new and more secure graphical password system called passpoints.

In passpoints system users create a fivepoint click sequence on a background image.Complex images an have hundres of memorable points,for ex:with 5 or 6 click points one can make more passwords than 8-character unix-style passwords.Some tolerance region is set for each password because the tolerance [2] gives a margin of error around the click point in which the user's click is recognized as correct.

With the help of passpoint-style graphical passwords human seeded attacks have been used by human computed data which is further used to make easier and efficient attacks. The attacker require such attacks to collect the adequate "human computed "data for an image targeted [1],[9].Evaluating and introducing a set of purely automated attacks against the passpint-style graphical passwords. Users are more interested in choosing a click points based on some hypothesis that hoosing a click points in that areas of image where the user attention is accordingly drawn towards i.e,five click points in a straight line is called click order patterns.

Dictionaries where generated from the graphical passwords for the use in a dictionary attack.A successful attack must be able to efficiently generate a dictionary containing highly probable passwords.the cost of the dictionary depends on the different background images.

II. LITERATURE REVIEW

2.1 RELATED WORK

We concentrate on click-based graphical password schemes where a user cliks on a number of set points in a background image and work is related to guessing attacks on graphical passwords.

In Blonder's proposal users click on a set of predefined regions [3].

In Dhamija and Perrig's proposal user is asked to select a number of images from a set of random pictures.

Passpoints allow users to click a sequene of some points anywhere on an image with a error tolerance.e,error tolerance can be st to as p=4.An attacker ould predict hot spots by using image processing toole for guessing passpoints passwords and for other images their method guessed 9.1% and 0.9% pf passwords on two images using an dictionary attack 2^{35} entries compared to password space 2^{43} password.

Some of the click-order patterns evaluated with human seeded attacks is DIAG and other is LINE and other click based graphical password schemes CCP [7] and PCCP [6].

The major advantage of passpoints is its large password space over alphanumeric passwords.The large password space is significant because it reduces the gueesability of passwords

2.2 Survey

Recognition based systems

Recognition based systems also known as cognometric systems or search metric systems generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images. Recognition based systems have been proposed using various types of images. Phishing attacks are somewhat more difficult with recognition-based systems because the system must present the correct set of images to the user before password entry. Shoulder-surfing seems to be of particular concern in recognition-based systems

when an attacker can record or observe the images selected by users during login [6].

For PassFaces, the analysis of user choice by Davis et al. [10] showed that users tend to select attractive faces of their own race; and that users selected predictable sets of faces such that an attacker knowing one face could determine the face most likely to be selected as the next password part. Because users tend to select predictable images, successful dictionary attacks may be expected, as well as personalized attacks, e.g., if attackers know a user's race or gender. Davis et al. [10] guessed 10% of passwords created by male participants in 2 guesses. A major conclusion was that many graphical password schemes, including Faces, may require "a different posture towards password selection" than text passwords, where selection by the user is the norm. As noted in Section V (which also mentions user choice issues in the Story scheme [10]), a phishing attack on PassFaces requires a MITM attack

Recall based systems

In this section two types of picture password techniques used reproduce a secret drawing and repeat a selection. In these systems, users typically draw their password either on a blank canvas or on a grid i.e, DAS technique proposed by Jermyn [4].

Passlogix [11] has also developed several graphical password techniques based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as a password. Other password options include picking a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only provides a limited password space and there is no easy way to prevent people from picking poor passwords (for example, a full house in cards).

2.2 Graphical password Attacks

Brute Force Attack

This type of attack uses an algorithm that produces every possible combination of words to break the password. Text-based password contains 94^N number of space where 94 is the number of printable characters (including space) and N is the length. This type of attack has always proven successful against text-based password because of its ability to check all possibility within the length of the password. As such, users are advised to select a stronger and complex password to prevent discovery from brute force attack (Eiji Hayashi, 2008). However, GUA proves to be more resistant to brute force attacks since the attack software needs to produce all possible mouse motions to imitate passwords especially when trying to recall the graphical passwords. One of the reasons that helped is the large password space present in most graphical passwords techniques which is not available in the textual variant [5].

Dictionary Attack

This ingenious attack uses words found in the dictionary to check if any were used as passwords by the users. Many users' uses weak passwords which make it easier for attackers to guess the password using the graphical dictionary attack[6]. Because of graphical password method of using mouse input type recognition, using dictionary attack on GUA would be a waste of time.
Dictionary attacks against recognition and cued-recall graphical password systems require more effort up-front than against text passwords or recall-based graphical passwords, since attackers must first collect one or more of a set of images. Images gathered for one system will not help attacks on a second system, unless both systems use the same image set. During recall, it is more difficult and complex to use the automated dictionary method to produce all possibility of a single user click of an image than a text-based attack [6-8].

Spyware Attack

This attack uses a small application installed on a user's computer to record sensitive data during mouse movement or key press. This form of malware secretly store these information and then reports back to the attackers system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords. Even if the movement is recorded, it is still not accurate in identifying the graphical password. Other information is needed for this type of attack namely window size and position as well as the timing [9].

Shoulder-Surfing Attack

As the name implies, passwords can be identified by looking over a person's shoulder. This kind of attack is more common in crowded areas where it is not uncommon for people to stand behind another queuing at ATM machines. There are also cases where ceiling and wall cameras placed near ATM machines are used to record keyed pin numbers. The best way to avoid pin numbers being recorded or remembered by attackers is to properly shield the keypad when entering the pin number [10-12].

Guessing attack

Since many users try to select their password based on their personal information like the name of their pets, passport number, family name and so on, the

attacker also tries to guess passwords by trying these possible passwords. Password guessing attacks can be broadly categorized into online password guessing attacks and offline dictionary attacks. In an online password guessing attack, an attacker tries a guessed password by manipulating the inputs of one or more oracles. In an offline dictionary attack, an attacker exhaustively searches for the password by manipulating the inputs of one or more oracles (Roman, 2007).

III. TERMINOLOGIES

Some of the hypothesis where used to choose a passwords which consists of click points i.e distinguishable points and calculable points with corner detection and centroid detection [1].Corner detection contains intersection of the two edges and centroid detection contains objects in the center[1].

3.1 Dictionary Generation Algorithm

Inputs:permutations,digraph

Output:valid passwords generated

Step 1: sub dictionary is generated and is set to Null for (Digraph is set with vertices 1 to n)
Step 2: paths are allocated with some path finding algorithm with inputs sub dictionary, path of length
Path is a set of paths of lengths i.e., passwords
Step 3: sub dictionary is a set of combination of paths
Step 4: end of for statement
Step 5: return back to sub dictionary

In the above algorithm if a attacker plans to generate a dictionary which may consist of subsets of all the permutations involved which must satisfy the some predefined conditions one proposed approach is to generate only those permutations that satisfy the conditions heuristically.
This algorithm generates a subdictionary for a subheuristic such as right-to-left and left-to-right clikoder pattens.
The advantage of this algorithm is it increased the validity of passwords and long-term memorabiliy. [7]

3.2 Path Finding Algorithm

Inputs: length, source, digraph dg

Outputs: combinations of all subdictionaries is a final attack dictionary

Step 1: subdictionary sd is set to Null
Upon termination sd is a set of paths of length
Step 2: for all the nodes nearby neighbor S should belong to the source.
Step 3: neighbors S would be the set of neighbos of node S
Step 4: if the length is less than 1 then paths go back to the step1
Step 5: path prepends source
Prepend(paths ,S) pepends node S to path p
Paths is set with source and node S
Step 6: sd is the combination of all paths

Finding paths is a recursive function which finds all paths of defined length from the node in digraph From this algorithm the edges can be defined by the points in an image and distance between the image can be measured and the creation time for attacks depending on the number of dictionary entries.
Finding paths in an image can be identified by applying kruskal's algorithm as a proposed method o some more algorithms.

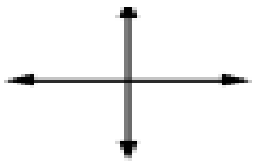
3.3 Different Click-Order patterns

DIAG pattern

DIAG is a lazy variation. It includes sequence of any five click-points that can be in horizontal and vertical direction. DIAG dictionary is a set of four union sets of passwords containing right to left, left to right, top to bottom, bottom to top.

LINE pattern

LINE pattern is a super-lazy variation.It includes sequence of any five click-points that can be in horizontal and vertical line



IV. PASSPOINT METHOD

To improve upon the shortcomings of the Blonder Algorithm, in 2005, PassPoint was created Passpoint was able to fill in the gaps left by blonder. In this case the image could be any natural picture or painting as well as rich enough so as to have several possible click points. Apart from this the image is not secret and has no other role other than that of assisting the user to remember the click point. Furthermore it is not as rigid as the blonder algorithm which requires

the setting of artificial predefined click regions with well-marked boundaries.[8]

The authentication process involves the user selecting several points on picture in a particular order. When logging in, the user is supposed to click close to the selected click points, within some (adjustable) tolerance distance, for instance within 0.25 cm from the actual click point Studies indicate that when using the PassPoint system users were easily able to quickly create a valid password. They found it much harder to know their passwords compared to alphanumeric users, hence they had to take a lot more trials and more time to complete the process. Comparatively the login time, in this method is longer than that of the alphanumeric method

CONCLUSION

Finally, purely automated attacks are arguably much easier for an attacker to prepare especially if large image datasets are used. Corners and centroids of images might be extracted, and used to build a click-order heuristic graph. Finally, our attacks could be used to help inform more secure design choices in implementing Pass Points-style graphical passwords. Pass-points passwords are most robust than text passwords against multiple password interference.

REFERENCES

[1] Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe "Purely Automated Attacks on PassPoints-Style Graphical Passwords"

[2] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "Authentication using graphical passwords: Basic results,"in Proc. Human-Computer Interaction Int. (HCII), Las Vegas, NV, 2005.

[3] G. Blonder, "Graphical Passwords," U.S. Patent 5559961, 1996.

[4] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Computer Security Applications Conf. (ACSAC), Tucson, AZ, 2005.

[5] Hayashi, E. and N. Christin, Use Your Illusion: Secure Authentication Usable Anywhere, in Proceedings of the 4th symposium on Usable privacy and security (SOUPS). 2008,ACM.

[6] Chiasson, S., et al., Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. ACM,2009

[7] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle" Graphical Password Authentication Using Cued Click Points"

[8] Arash Habibi Lashkari, Samaneh Farmand1"A new algorithm on Graphical User Authentication(GUA) based on multi-line grids

[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A second look at the usability of click-based graphical passwords," in Proc. 3rd Symp.Usable Privacy and Security (SOUPS), Pittsburgh, PA, 2007.

[10] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in 13th USENIX Security Symposium, 2004.

[11]Passlogix, "www.passlogix.com," last accessed in June 2005.

★★★