ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (57-63), Month: July - September 2014, Available at: www.researchpublish.com

GRAPHICAL PASSWORD

R. Nithya[1]

[1] Student, Department of Computer Science Engineering, Saveetha School of Engineering, Saveetha University, Chennai– 602 105, India

Abstract: **As the globe is growing so fast it is necessary that we have to be secure. The modern world is highly computerized and hence forth we have to move on with it. In order to increase the security usually the password technique is used. The commonly used password is of the type text. Still there are so many disadvantages in it. Here, we present to you a new password technique of the type Graphical which deals with authentication through image. The graphical data represents billions of bytes of information and thus provide lot of password space. Thus graphical password provides a way of making more human friendly passwords while increasing the level of security.**

Keywords**: Password Technique, Text Password, Graphical Password.**

I. INTRODUCTION

Passwords are the foremost unremarkably used technique for distinctive users in communication systems and laptop . Typically, passwords are strings of digits and letters, i.e., they're alpha-numeric. Such passwords have the disadvantage of being arduous to recollect. The passwords are expected to fits two conflicting requirements:

1. Passwords should be easy to recollect, and also the user authentication protocol should be executable quickly and simply by humans.
2. Passwords should be secure, i.e., they must look random and may be arduous to guess; they must be modified frequently, and may vary on different accounts of the same user. They must not be written down or stored in plain text.

Here we have a tendency to discuss graphical passwords, that include some actions that the user performs on a picture. Such passwords are easier to recollect, but they are susceptible to shoulder surfing. We present a number of graphical password schemes that provide resistance to shoulder surfing.

II. TEXT PASSWORD

Alpha-numeric passwords were initial introduced in the 1960s as a solution to security problems that became evident as the first multi-user operating systems were being developed. As the name indicates it is known as alpha-numeric password is simply a string of letters and digits. Although virtually any string will function a password, these passwords only offer sensible and good security as long as they're difficult enough so they cannot be deduced or guessed. Normally used guidelines for alpha-numeric passwords are:

- The password should be a minimum of eight characters long.
- The password should not be easy to relate to the user (e.g., last name, birth date).
- The password should not be a word that can be found in a dictionary or public directory.
- Ideally, the user should combine upper and lower case letters and digits.

Since the best password would be a totally random one, individuals have devised ways to form pseudo-random passwords. One such technique is to take a common word and perform certain actions on it.

Using the word Creative as an example, users usually produce passwords like.

- CrEaTiVe (by alternating upper and lower case),
- eViTaErC (by reversing the string),
- aCEriTVe(by shuffling the string),
- 3a8tive (combining numbers and letters).

However, the better the password is, difficult to remember.

Pit Falls Of Text Password

We use passwords for opening our e-mail box, withdrawing cash from an ATM, accessing our web-based e-mail account, into our office Intranet, logging-in to our favorite web sites, etc. When the mind is already flooded with many tasks, remembering these passwords a laborious and unnecessary job. To lighten this burden, most people take recourse to some tiny tricks like choosing simply recallable password strings, as an example, selecting the name of a relative/friend as password, keeping a similar password for all accounts and services, noting down passwords in a diary the like.

The top twenty passwords are (in order): abc123, 123abc, myspace1, password1, password, blink182, qwerty1, creative, superman1, baseball1, football1, iloveyou1 soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, 123456, and monkey. The most common password, "password1," was used in 0.22 % of all accounts. The frequency drops off pretty quick after that: "abc123″ and "myspace1″ were only used in 0.11% of all accounts, "soccer" in 0.04 % and "monkey" in 0.02%.

Another disadvantage of alpha-numeric password is that the lexicon attack. Because of the difficulty in remembering random strings of characters, most users tend to choose on a common word, or a name. Unfortunately, there are many tools that permit a individual to crack passwords by automatically testing all the words that occur in dictionaries or public directories. This attack can typically not uncover the password of a predetermined user; however studies have shown that this attack is sometimes productive to find valid passwords of some users of a given system.

III. GRAPHICAL PASSWORD

The idea of graphical passwords, initially represented by Greg Blonder [G. Blonder, Graphical Passwords, Patent (1996)] , is to let the user click (with a mouse or a stylus) on some chosen regions in a picture that appears on the screen. Because human beings live and interact in an environment wherever the sense of sight is predominant for many activities, our brains are capable of processing and storing massive amounts of graphical data with ease. While we may find it very hard to remember a string of fifty characters, we are easily able to remember the faces of individuals, places we visited, and things we've seen. This graphical information represents immeasurable bytes of data and thus provides a massive password spaces. A graphical password is an authentication system that works by having the user choose from images, in a very specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes known as graphical user authentication (GUA).

Advantages Of Graphical Password

A graphical password is simpler than a text-based password for many individuals to recollect. Suppose an 8-character password is necessary to gain entry into a specific computerized network. Instead of w8KiJ72c, for eg., a user may choose pictures of the earth (from among a screen packed with real and fictitious planets), the town of Nice (from a map of France), the country of France (from a map of the world), a white stucco house with arched doorways and red tiles on the roof, a package of Gouda cheese, a bottle of fruit crush, a green plastic cooler with a white lid, and a pink drinking cup with very little green stars around its upper edge and 3 red bands around the middle.

Graphical passwords may offer better security than text-based passwords because many of us, in a attempt to memorize text-based passwords, use plain words (rather than the suggested jumble of characters). A dictionary search can often hit on a password and permit a hacker to gain entry into a system in seconds. but if a series of selectable pictures is used on successive e screen pages, and if there are several pictures on every page, a hacker must try every possible combination at random. If there are 100 pictures on each of the 8 pages in an 8-image password, there are 1008, or 10 quadrillion, thus the possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of every image until the presentation of the next page, it might take several years to break into the system by hitting it with random image sequences.

A Simple Graphical Password Scheme

This example, whereas terribly unsophisticated, it illustrates how a simple graphical password matches the security of its alpha-numeric counterparts. Therefore to login, the user is required to click within the four circled red regions in this image. The user selected these regions once he or she created the password. The selection for the four regions is arbitrary, but the user can decide places that he or she finds simple to recollect. The user can introduce his/her own photos for creating the graphical passwords and also for stronger security, more than four click points could be chosen.

Perhaps the biggest drawback for current graphical passwords is that the shoulder surfing problem. Although graphical passwords are difficult to guess, and a person who gets to observe a few login sessions could, depending on the scheme, eventually figure out the password. Thus the above example reveals the password to anybody watching the login session.

Due to this vulnerability to shoulder surfing, it would appear that the graphical passwords could never be used in environments wherever view of the screen is not exclusive to the person logging in. However, we have identified that by applying the concept of challenge response it is possible to create schemes that counter the shoulder surfing problem.

IV. THE SHOULDER SURFING PROBLEM

As the name implies, shoulder surfing is watching over people's shoulders as they process data. Examples include observing the keyboard as a person types his or her password, when they enters a PIN number, or views personal information because of their graphic nature, nearly all the graphical password schemes are quite vulnerable to shoulder surfing. Most of the existing schemes simply circumvent the problem by stating that graphical passwords should only be used with hand-held devices or workstations set up in such way that only one person can see the screen at the time of login.

While it is usually possible to make sure that there are no people looking over one's shoulder at the time of login, the value of graphical passwords as an alternative to alpha-numeric passwords diminishes somewhat if they can only be utilized in environments set up to prevent shoulder surfing. To resolve this here we introduce 3 schemes.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (57-63), Month: July - September 2014, Available at: www.researchpublish.com

Step [1]. Challenge response authentication
Step [2]. Triangle scheme
Step [3]. Movable frame scheme

Challenge Response Authentication

Challenge response authentication enables an entity (B) to prove an entity (A) that (B) knows a secret shared by both (A) and (B). However, this proof of knowledge is finished in such a way that the actual secret is not revealed to any third party who may be listening in.

Typical Challenge Response Session

User (B) sends a login request to server (A), which in turn sends back a random number r. Thus the challenge for the user is to evaluate f(n+r). The user's identity is accepted if the last message received from (A) corresponds to f(n+r). A user who knows n can easily compute f(n+r). On the other hand, an eavesdropper who captures r and f(n+r) cannot deduce n in a realistic amount of time. Additionally, the use of a random number r prevents the reuse previously

V. ADAPTING CHALLENGE RESPONSE TO GRAPHICAL PASSWORDS

The challenge response authentication that we just described is not intended to be used directly by humans to authenticate themselves to a system, because it requires many calculations to evaluate an alpha-numeric one-way function for some random value. However, we can use the human ability to process graphical data. The goal is to create a graphical one-way function that will prevent an adversary from obtaining the secret even if he or she has full view of the value of the graphic one-way function.

As the figure illustrates, all the adversary would see is r and f(n+r). And although f(n+r) is publically available, the password n is required to solve the next random challenge, unlike the typical challenge response, the password n is not alpha-numeric but rather a geometrical pattern used to evaluate r. Similarly, n and r are graphical. The analysis of f(n+r) is done without computation and can be easily performed by a user in a reasonable amount of time. Instead of sending a random number for each challenge, we can obtain the same functionality by performing certain random operations on a picture (e.g., rotation, changes in position, perspective and shading).

VI. TRIANGLE SCHEME

The system randomly scatters a set of N objects on the screen. In practice, the number N could be a few hundred or a few thousand, and the objects should be different enough so that the user can distinguish them. In addition, there is a subset of K pass-objects previously chosen and memorized by the user. At login the system will randomly select a placement of the N objects. However, the system will randomly chooses a patch that covers half the screen, and randomly places the K chosen objects in that patch. To login, the user must find 3 of the pass-objects and click inside the invisible triangle created by those 3 objects. This is equivalent to saying that the user should click inside of the convex hull of the pass-objects that are displayed. In additionally, for each login this challenge is repeated a few times using a different display of some of the N objects. Therefore, the probability of random clicking within the correct region in each challenge is very low.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (57-63), Month: July - September 2014, Available at: www.researchpublish.com

The number of possible passwords is the "binomial coefficient" (choose any K objects among N). When N = 1000 and K = 10, the number of possible passwords is hence approximately $2.6 * 10^{23}$. This is a little more than the number of alpha-numeric passwords of length 15, Then 36^{15} ($2.2 * 10^{23}$). Having N = 1000 objects is not unreasonable (compare with the "Where is Waldo" puzzles, where there are typically tens of thousands of little persons in a picture). Moreover, one can expect a user to choose the K objects fairly randomly; or, at least, an attacker (especially a computerized attacker) cannot predict much about which K objects a user will select. On the other hand, the large number of possible alpha-numeric passwords 36^{15} ($2.2 * 10^{23}$) is an illusion: users do select alpha-numeric passwords randomly at all.

After an attacker sees one click on the screen from the user, the attacker learns that the K pass-objects are such that their convex hull contains the click point. These rules out all the K-tuples that do not have the click point in their convex hull. However, when N = 100 and K = 10, the set of ruled-out K-tuples is at least > 2 * 1020, which is overlarge to be remembered in any computer memory (compare e.g., with the Avogadro number NA ($6 * 10^{23}$ atom/mole).Hence the attacker can only remember a negligible amount of what he learns in each shoulder surfing result. As a consequence, the attacker cannot accumulate knowledge of the user's password. This shows that an exhaustive-search attack is physically infeasible; moreover, when passwords are chosen truly, exhaustive-search attacks are the only possible attacks.

An improved version of this system would display only objects (N / 2 N) among which are pass-objects (with 3 K). This simplifies the login of the user, while making attacks .

VII. MOVABLE FRAME SCHEME

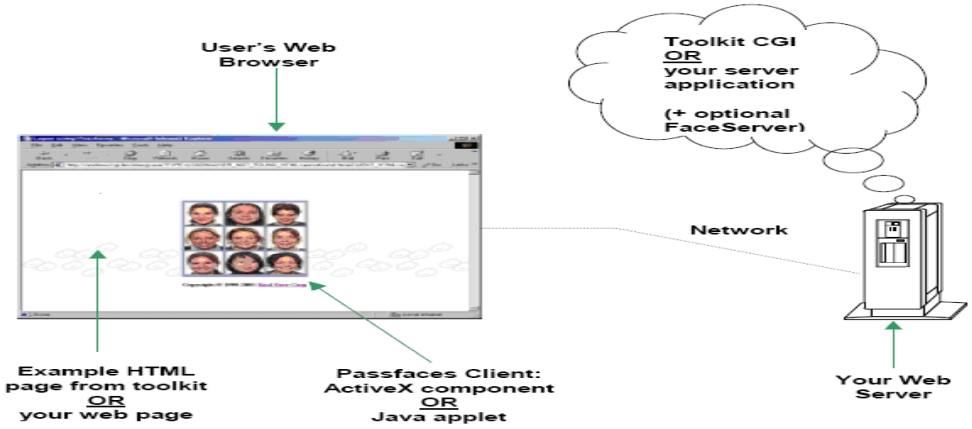
Using the same ideas and assumptions as in the previous scheme, the user must now locate 3 out of K pass-objects. This time however, only 3 pass-objects are displayed at any given time and only one of them is placed in a movable frame as depicted below. Which pass-object is displayed within the frame is completely arbitrary. The task of the user is to move the frame (and the objects within it, like a tape) by dragging the mouse around the frame until the pass object on the frame lines up with the other two pass-objects. As before, this procedure is repeated a few more times to minimize the like hood of logging in by randomly moving the frame.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (57-63), Month: July - September 2014, Available at: www.researchpublish.com

VIII. FACE PASS

Another scheme of graphical passwords is the Pass face that has been advertised all around the globe through various media. All of us have an innate capability to an instantaneously recognize pictures. If we were shown an old group-photograph and asked to identify a individual whose face we already know, most of us would point our finger at the proper face. It is widey accepted that people have a remarkable ability to recognize human faces.

Pass faces is a unique authentication system offering simple, easy and secure logon. It is a graphic verification technology that uses faces instead of everyday pictures. This patented approach, cognometrics, takes advantage of the brain's innate ability to recognize and recall faces. And since we "never forget a face", password resets are just virtually eliminated



This feature is skillfully deployed in creation of the authentication tool called the pass face, instead of the word-based entry pass, here we have a `face'-based entry pass. Here the pass phrase is not a string of alphanumerical characters however a string of face pictures. You can choose a picture combination and whenever you are attempting to access a service based on this authentication method, the system will show you a set of faces from which you need to select the ones that belong to your password string.

Other Solutions

There are other kinds of passwords like biometrics and eye password. An eye password requires your physical presence before the eye detector. Moreover the cost of the eye detector is on the higher. So practically it is not possible for all kind of users to authenticate through eye passwords. Graphical passwords are of no cost which makes users feel more comfortable.

Biometrics is also of the similar type rather than the physical presence the physiological or behavioral characteristics of the person concerned is studied and authenticated. This needs a lot of work to be done in order to process the activities of the person and make sure his authentication. Thus Graphical passwords are easier to be handled as at a low cost.

IX. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have got conducted a comprehensive survey of existing graphical password techniques. Although the Main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to interrupt.

Graphical passwords using the traditional attack strategies like brute force search, dictionary attack, or spy ware. However, since there is not yet wide preparation of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.

Overall, the present graphical password techniques are still immature. Much more research and user studies are required for graphical password techniques to achieve higher levels of maturity and usefulness.

REFERENCES

[1] A S. Patrick, A C. Long, and S. Flinn, "HCI and Security Systems", presented at Cm, Extended Abstracts (Workshops). Ft Lauderdale, Florida, USA, 2003.

[2] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of Th ACM, vol. 42 pp. 41-46, 1999.

[3] R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.

[4] A. Perrig and D. Song, "Hash Visualizations: A New Technique To Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," inProceedings of Midwest Instruction and Computing Symposium, 2004.

[6] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Hman Factors in Computing Systems (CHI), Vienna, Austria: ACM, 2004.

[7] L. Sabrado and J. C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002.

[8] S. Man, D. Hong, and M. Mathews, "A Shoulder-Surfing resistant graphical password scheme," in Proceedings of International Conference on security and management Las Vegas, NV, 2003.

[9] D.Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium, San Diego, CA, 2004.

[10] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware", in Proceedings of International Conference on security and management Las Vegas, NV, 2003.