Mitigating Attacks on Authentication using Graphical Passwords

Divesh Patil[1], Atiya Kazi[2], Akshay Raut[3] ,Shahid Mukadam[4], Abhishek Ghanekar[5]

[1345] Student, Dept. of Information Technology, FAMT, Ratnagiri
[2]Asst.Prof, Dept.of Information Technology, FAMT, Ratnagiri

Abstract - *User Authentication is mandatory in the field of Information security to guarantee that the individual is who he or she claims to be, but it neglects the access rights of the individual. Human and social factors are the weakest links in the Information security chain. Problem lies with users who are unable or reluctant to conform to security protocols. Prevailing Authentication methods have certain boundaries. Biometric authentication necessitates users to reveal their individual information for authentication. Disadvantages of Biometric authentication are: overpriced, disability issues, false positives and negatives etc. In token-based authentication, Operators must bring a symbolic token to be offered for verification every time. Text passwords are handy since users simply have to recall them, but they are absolutely vulnerable to dictionary attacks, brute force attacks. A substitute to text based password is graphical and image based passwords. In this paper, we conduct a comprehensive survey of the prevailing graphical and Image based authentication techniques and see how they provide better alternatives to current authentication schemes.*

Key Words: Authentication, Security Attacks, Graphical Password

INTRODUCTION

In the current scenario, web threats are changing. Decision makers have the task of understanding the nature of the threats in software world. Hence the web, network and application security face some extremely difficult issues. Despite the growing array of threats, many organizations are not taking appropriate steps to safeguard their corporate networks, applications or ID/Passwords. This has led to the problem of memorability. Wireless Internet Service Providers implemented web based authentication mechanism which has become widely popular with customers for its simple and efficient UI[1]. Authentication is a direct need of each and every organization and so it is becoming a chief objective for an organization not because it handles with security threats only but also because it develops policies, procedures and mechanisms that provide organizational, corporeal and rational security. On every occasion an individual requests an entree to a pool of resources, either to use or to update, then to validate such an individual is referred to as authentication [3]. The software industry has created an array of identification and authentication technologies like userID/Passwords, One Time Password, Biometrics, Smartcards, Kerberos, Secure Socket Layer (SSL), Security Assertion Markup Language (SAML), OpenID, Lightweight Directory Access Protocol (LDAP) and CardSpace to address varying business and security requirements [5]. Each organization makes use of one or more of these technologies to secure information against ill use and non-trusted access. In any company's private network, users are granted admittance only when they provide their correct access information (e.g. user name & password). In other cases, if a person can prove that who he is, also knows something that only he could know, it is reasonable to think that a person is he who claims to be. The purpose of own authentication is to guarantee that the extracted services are being retrieved only by a legitimate user [2]. The world today is a melting pot of thefts and terrorism. This makes secure and robust authentication more important for an organization to provide an accurate and reliable means of communication. Many electronic commerce (e-commerce) web sites use authentication interface as a graphical security interface. In many applications such as e-voting and Internet banking, it is not necessary to know who an entity actually is, but to be sure that he/she retains the appropriate rights to perform the chosen action. Every user of such applications wants reassurance that what he sees on the computer screen is the actual content sent from a reliable supplier or demonstrated by a trusted application. This is exactly the purpose of authentication and authorization infrastructures. In b2c e-commerce applications, it is not mandatory to ask someone "Who are you?" but rather "Are you allowed to perform a certain request"[4]. Different administrations have dissimilar authentication requirements and so they hire different verification techniques. But whatever the authentication technique is employed, the foremost goal of authentication is to expansion the level of guarantee of legal users and to stop the phonies from accessing the system. This paper attempts to explore several newbies in graphical authentication world. The methods discussed in this paper are proven to be more reliable than the customary authentication systems used so far and the secret information will be harder to steal.

2. ATTACKS ON PASSWORDS

2.1 Brute force attack: It is a computerized process used by rookies as a trial and error method to crack a naïve person's user name, password, credit card number or cryptographic key. A standard brute force attack tries a single user name against many combinations of possible passwords. On the other hand, a reverse brute force attack tries several possible user names against a known password. When a predicted password allows access to the system, the brute force attack has been effective and the aggressor has gained admittance to the account. Brute Force methods are extremely popular and often positive in schemes with many user accounts.

2.2 **Insufficient authentication:** When a website allows an attacker to contact with sensitive content or functionality without bothering proper authentication, it leads to insufficient authentication. A good example of this is a certain web application may have been designed with administrative functionality to find the location of the root directory using statements like "../admin/..". This directory is usually hidden on the original web site, but still an attacker can access it using a standard web browser and some easy backtracking commands.

2.3 **Weak password recovery:** Sometimes a website authorizations users to illegally obtain, change or recover another user's password. Traditionally, web site authentication methods ask users to select and remember a permanent password. Ideally only the person must know the password and recall it precisely during log in. But with the passage of time, a user might forget the password. Also he might be confused if he visits many websites and stores a different password every time. In such cases, a website offers Password Recovery Validation. During this, an attacker can outwit the recovery mechanism. For instance, the information which validates a user's identity can be easily guessed or evaded. Password recovery systems are highly susceptible to brute force attacks. An attacker may make use of the inherent system weaknesses or easily guess the secret questions. Example of automated password recovery process where the user answers a " secret question "or provides a " hint "during registration that will help the user remember his forgotten password.

2.4 **Shoulder surfing attack:** The attacker observes the password from a safe distance by using spy cameras to capture the user entering the password.

2.5 **Phishing attack:** It tries to illegitimately and deceptively acquire sensitive information i.e. user name, password and credit card details using bulk or spam mails.

2.5 **Reconnaisance attack:** The act of learning sensitive information which is thrown away by the user but is publicly available.

3. GRAPHICAL PASSWORD AUTHENTICATION

Graphical password is an authentication system that asks the user to select from images, in a specific order, from a graphical user interface (GUI). Existing graphical password schemes can be categorized into following categories:

1. Recall-based
2. Recognition-based
3. Cued-recall

In the recall-based scheme, a user is asked to reproduce a pre-drawn sketch with an input device such as the mouse or stylus on a grid. Recognition-based scheme requires the user to learn by rote an assortment of images during password formation, and then recognize his own images from among a number of distractions during authentication. Cued-recall scheme, intends to retain the memory load on users. It generally offers a background image and the user must remember and target precise positions on the image with a minor tolerance level.

4. DESIGN AND IMPLEMENTATION ISSUES OF GRAPHICAL PASSWORDS

4.1 Security

An important security goal of authentication mechanisms is to make the most of the actual password space; we would like the actual password space to comprise as much of the academic password space as possible. Meanwhile the actual password space is determined by user behavior, the strategy of a scheme involves usability as well. Ideally, passwords should be locked without foregoing the usability of the system. In exercise, growing one often reduces the other, so typically a middle-ground must be found where both the safekeeping and usability of the system are tolerable. Events of the actual password space are vague guesses. One tactic that may help is to distinguish classes of passwords that have advanced probability of being chosen by users. In this case, a closeness resolve may be useful.

4.2 Usability

One of the key arguments for graphical verification is that images are much easier to recall than text strings. Some research papers presented preliminary user studies to support this. However, recent user studies contains only a few users. But it is still difficult to assume that graphical passwords are easier to recollect than text based passwords as such there is no evidence. A major complaint among the users of graphical authentication procedure is that it takes too much time for the registration process and log-in process [7]. For example, in the registration phase, a user picks a few images from a grander image set. Then in the authentication phase, he identifies a few selective images by skimming through all the displayed images. This process is long and tedious. Due to this users opt for text based passwords. And also many users are not aware of the graphical passwords trend as it is fairly new in the security world.

4.3 Reliability

The key issue for recall-based methods is the consistency and precision of user input credit. The tolerances in graphical authentication schemes have to be fixed judiciously. In case the tolerances are overly high then it may lead to many false positives while if they are too low, it may lead to many false negatives. Additionally, if the program is more fault tolerant, then it will be exposed to attacks.

4.4 Communication and storage

Graphical verification schemes need much more space for storing than text based passwords. A major collection of images have to be maintained in a centralized storage database. The delay in loading or transfer of images is also a concern for graphical authentication schemes. Particularly for recognition based techniques in which many images may need to be displayed for each round for providing proof in the authentication process.

5. ALGORITHMS FOR GRAPHICAL PASSWORDS

Several algorithms are currently in use for graphical authentication. A few of them are discussed in this section.

5.1 Draw A Secret (DAS)

It is a pure recall based technique which makes a user to draw the pattern correctly. This is accomplished without getting any hint from the system. The technique makes use of a grid of size G*G. Each cell has coordinates (x,y) assigned to it. The created pattern is stored in the form of sequence of coordinates such as,

(2,2), (3,2), (3,3), (2,3), (2,2), (2,1)

During authentication, the user is asked to recreate the pattern in one stroke as it was drawn in registration phase without lifting the digital pen. On successful pattern matching, a user will be authenticated. This technique is quite popular among mobile applications which employ a pattern lock system during unlocking the phone.

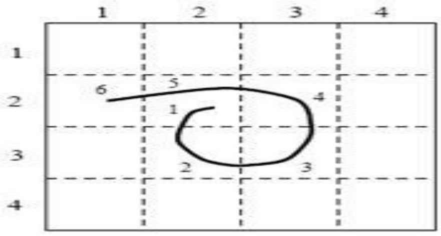

Fig -1: DAS

5.2 Grid Selection Algorithm

Grid selection algorithm is similar to previously explained pure recall based authentication technique. It overcomes the short-comings of password space and stroke count which were seen in the previous case. Initially, it is mandatory to select a small region from a large rectangular grid as the first step. Once the region is zoomed in on selection, the user is prompted to draw the password pattern that he must remember for future authentication. An example of one such scheme is shown in the Figure 2.

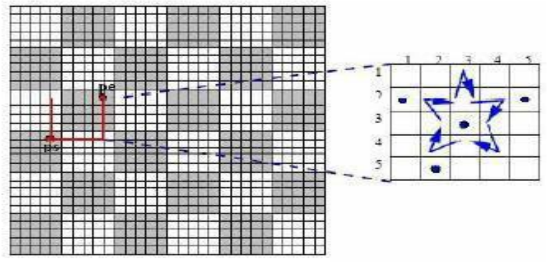

Fig -2: Grid Selection

5.3 PassPoint Algorithm

The PassPoint Algorithm is also known as cued recall based technique. The scheme allows a rich natural image to have many imaginable click points. Actually the image is just to provide a hint to the user in recalling the click points. During login, the user selects the click points in the same order as in Registration phase with some adjustable tolerable distance such as 0.25 cm from the actual click point.

Fig -3: PassPoint Algorithm

The user will click on the predefined image at predefined region. This makes the system more secure to random shoulder surfing attacks.

6. COMPARISON OF ALGORITHMS

The image based authentication scheme is where a group of images are provided to the user during registration phase. Among these the user has to select a set of images which he/she can identify and use them in future. Then to get authenticated the user has to recognize and choose the previously selected images. This scheme is helpful to user as it is easy to remember but not completely secure as it is vulnerable to guessing attacks etc[6]. Initially the user allowed selecting a set of images from a group of images that are displayed by the system during registration phase. The same set of images is to be identified and chosen by the user to get authenticated. The drawback in this scheme is tracking the set of selected images by user in image database can be complex and time consuming process.

Another authentication scheme that deals with shoulder surfing problem is, during registration, the user is allowed to choose set of objects among the displayed group of objects to form a convex hull by the system. To get authenticated to the system, the user has to recognize and click on those objects such that a structure of convex hull is formed. On increasing the selection of number of objects the length of password increases which is more secure. The only drawback is it takes long period of time to log on to the system.

The next simple authentication system is where the user has to register using his/her details and an image of his own to the system. If the image matches with the one stored in the system, the user is authenticated. The images are not stored by the system. Byte wise information of images are read and hashed using a secure hashing function SHA-1.The user carries the image with him. To get authenticated user has to submit details and the image which is verified with the data stored in the database.

A new technique proposed by real user corporation is Passface. Initially to register, the user is provided with a group of images of human faces by the system where he/she has to select four of them which are familiar to them. These selected images form password during authentication. The process of authentication is as follows: the user sees a grid of nine images of human faces consisting of one that is previously chosen and the eight other images are not related. This step is repeated until the user recognizes all the four pre chosen human faces.

7. CONCLUSION

During the previous research the weaknesses of basic authentication schemes were discovered. A Survey conducted from traditional password and PIN authentication to image authentication system depicts that authentication systems have potential applications and these systems are well suitable to some extent but with some drawbacks. This paper shows various image authentication schemes which are more application oriented. Some algorithms offer high tolerance performances against manipulations that are specific to applications which include compression, geometrical transformations filtering etc. But even to be vigorous against a predefined set of manipulations an improved hash function technique with a combination of current techniques of transformation are to be proposed.

This paper also talks of advantages and disadvantages of different security techniques to the future developers with the purpose of showing a more intelligent technique using images. Daily new encryption techniques are budding hence fast and sheltered orthodox encryption techniques will always work out with high rate of security.

REFERENCES

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

[2] J. Birget,D. Hong, and N.Memon. Graphical passwords based on robust discretization. IEEE Transactions on Information Forensics and Security,1(3):395–399, 2006.

[3] H. Tao and C. Adams, “Pass-Go: A proposal to improve the usability of graphical passwords,” Int. J. Netw. Security, vol. 7, no. 2,pp. 273–292,2008.

[4] D. Umar, M.S.; Rafiq M.Q.;”Select-to-Spawn: A Novel Recognition based graphical user authantication skim”;Signal Processing Computing and Control (ISPCC), 2012 IEEE International Conference.

[5] Y.Zhu, and G. S. Owen, “Graphical Passwords: A Survey”, in Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE Computer Society, pp. 463-472, 2005.

[6] J. Thorpe and P. C. v. Oorschot, “Towards Secure Design Choices for Implementing Graphical Passwords,” in 20thAnnual Computer Security Applications Conference (ACSAC) Tueson, USA. IEEE, 2004.

[7] Information Security Principles and Practice by Mark Stamp - Second Edition.