ISSN 2250-3153

Web Authentication using Graphical Virtual Environment

Ms. Aruna Gupta

Asst. Prof. IT, JSCOE, Pune

Abstract- Authentication has become integral part of 90% of web sites. The major issue in web authentication is the limitation of human memory to remember the password string for longer period. Almost all websites are still using traditional recall-based textual password to identify their remote users. Vulnerability of this authentication mechanism due to the sophistication of online identity theft has led to the increased scope for the studies of recognition-based web authentication. This paper discusses the web authentication using graphical password built over the virtual environment. It examines the security threats associated with poor authentication practices of the Web and why is the need for businesses to strengthen web authentication. The paper also proposes a new approach for delivering one-time passwords using mobile phones.

Index Terms- Web authentication, Graphical password, OTP, Virtual environment.

I. INTRODUCTION

The purpose behind integrating authentication on a website may be to achieve Security, for Marketing/ advertisement, to establish Trustworthiness. This paper is focused on analyzing authentication of web sites which are highly sensitive towards security. Most of the financial or e-commerce websites are in search of improved web authentication mechanism for providing better security to their users. Security and trustworthiness are biggest challenges for such highly sensitive businesses running over public network. Security is important in authentication since breaking it, not only leads to financial losses but also in loss of user confidence in online services.

Every alternate website the user access asking for creation of credentials are resulting in selection of trivial password or choosing same password for lower as well as higher-security websites. Due to the lack of security implementation in lower-security websites, the attacker may easily get access to the user credentials which he may then use for accessing the user's account on highly secured website. E.g. - a user account on social site like www.ibibo.com may help attacker to exploit his bank account, provided that they have overlapping bases. Such cross-site account negotiation attacks are very common among the others.

Another reason that opens the door for the attacker is rare use of websites on which accounts are created. In such cases, often users are likely to forget their password. In response to solve this problem, they copy down the password somewhere, assuming it is the best place to keep their password safe!

This paper introduces an innovative way of web authentication using Graphical Virtual Environment. It is graphical password that helps the website users to efficiently create the secret information which is difficult for the attacker to guess. This leaves the human memory free to remember experiences and emotions; not engage in remembering random, critical string.

II. GRAPHICAL PASSWORDS

All the proposed and commercial graphical passwords can be categorized as recognition-based and recall-based. In first category mostly image or face is used whereas second uses grids to divide the picture.

Passfaces[1, 2]: In this recognition-based scheme, the user is required to select four images of human faces from a face database as the part of password generation. At the time of authentication, the user will face a grid of nine faces, consisting of one face previously chosen by him and rest eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for four rounds. The user is authenticated if he/she correctly identifies all the four faces. This technique assumes that people can recognize human faces easier than other pictures. The major disadvantage of Passfaces is that login process takes longer than text passwords. Also the passwords selected by users are very much predictable. Other problem is that it has smaller password space.

Similar kind of a system built for mobile devices was Imageshield introduced by Confident Technologies [6, 7].

GPEX[3, 4]: It is the password manager program implemented as a plug-in to the Firefox web browser. Passwords were generated by clicking five points on the picture which is divided into several small grids. The number of clicks to go is presented at the bottom of the image. Alternatively user can select five icon-size images out of set of images presented to him, by clicking on them to generate the password. The biggest problem with this scheme is the icon-size images are too small and shown plenty altogether, so memory stress required to recognize them. For the grid-based images, it is very difficult for the user to recall the click points over the image.

V-GO[5]: It allows a user to create a graphical password by navigating through an image. To enter a password, a user can click and/or drag on a series of items within that image. The scheme is lacking with the size of password space. In addition, a user chosen password might be easily guessable. Finally, the system requires users to precisely recall the authentication task, instead of relying on recognition.

III. PROPOSED SCHEME

Hackers are always moving a step ahead and developing new techniques to gain access to corporate information and we must be proactive in attempting to keep them away. Providing multiple layers of security is always the most effective way for securing any system. Such layered security can be provided through *multifactor authentication* [8]. Proposed here is a Multifactor Graphical Authentication Solution for web authentication using Virtual Environment.

There is a traditional trade-off associated with web authentication between security and usability. The websites that opts for security with the two-factor authentication scheme end up with the users facing complexity and paying high costs. On the other hand simple system like text password is not secured at all. Proposed system provides the balance between the two. It helps to build highly usable authentication system without compromising security.

When something is chosen out of interest rather than following the strict rules, recognition replaces the recall procedure. The main purpose of this scheme is to reduce the cognitive load of the user. The password is created by the using the sequence of actions performed by user within the virtual environment. Instead of remembering and typing a long and complex textual string, the user creates the password by clicking the graphical views. This scheme combines recognition-based system with the token-based system and optionally with the textual password. When the user faces virtual environment with which he is familiar, he can easily repeat the actions performed earlier. The reason behind the ease of usability is the selection of password is completely based on user's personal interest. The virtual environment provides hint at every step for completing the password as opposed to the text password where user gets no clue for recollecting the password.

Following sections describe the multiple factors of the proposed authentication system.

A. First Factor: Graphical Password

Recognizing picture is much easier than recalling non-dictionary words. This fact can be demonstrated with the example – Lets think of the game where no. of objects shown for a minute to a person and then he has to make list of their names. Doing this task is always better than reading a list with names of objects and then recalling and identifying the corresponding objects shown to you.

Password construction with Graphical Virtual Environment:

Virtual environment consists of virtual objects representing real life objects. The password generation process is divided into multiple categories. For example, selecting a bunch of flowers to insert into flower-pot, dialing a number on the mobile, setting time and date, selecting tour place for picnic, selecting favorite cricketer etc. For each category a screen is presented to the user where he may choose to interact or may skip the category. User has complete freedom of choosing the category containing objects of his interest. This helps him to remember the sequence of interactions for longer period. If user opts to interact then the interaction is converted into substring and added to the password being generated for the user. The substring generation on user interaction can be done as follows:

Formula: Action1(A1) Parameters List 1(PL1) #A2 PL2#.....An PLn

Example: SELECTbunch(1)#TRIPcity(5)#CRICKsachin

All the substrings are concatenated as shown above to form the password string. At the time of authentication, user is presented with the category screens he has interacted with. Along with that few more random category screens are inserted between them. This strategy helps in defending from the shoulder surfing attack. The observer will be confused with the different random categories inserted for every authentication. On the contrary, legitimate user recognizes the categories he has interacted with earlier and repeats the procedure to generate the password.

B. Second Factor: Mobile Phone as OTP device

In addition to user created graphical password, the presented scheme makes user enter one-time password (OTP) generated by software on his mobile to protect against Malware and Shoulder Surfing attack.

Use of an OTP device which generates OTP for the user to be entered on the website has four major issues: firstly, it will increase the cost of the system. Secondly, there is a risk of losing the device or it may be stolen. Third issue is that user has to carry this device wherever he goes as one never know when and where he may need it for web access. Fourth problem is that hardware tokens expire after a limited life span and then they need to be discarded and new ones have to be issued.

Alternative that provides solutions to these problems is to make use of user's mobile phone as an OTP device. It will save the additional cost of the device. Users are more likely to recognize the loss of their mobile phone rather than the loss of hardware token. This means that they are more likely to recover a misplaced mobile phone before finding a lost hardware token. Moreover, everyone generally carries mobile phones wherever they go. Also, mobile tokens are implemented using existing hardware; this minimizes negative externalities. An added benefit with such implementation is that this soft token embedded in mobile phone will not expire. This will help to improve customer satisfaction. As a result mobile phones are more reliable deployment method than hardware tokens.

In most of the recent multifactor implementations, website sends an OTP to the user's mobile phone via SMS text message. The criminals use various technologies to intercept the text messages and extract the OTP to use it for authenticating their fraudulent transactions. This is the well-known man-in-the-middle (MITM) attack. Furthermore, the SMS text messages are often sent in clear text form and anyone having access to the mobile phone can read the message. To protect OTP against the MITM, the proposed scheme provides the generation of OTP on mobile device itself to avoid transferring it over insecure network. The OTP can be calculated on the basis of following factors:

Exact date and time of day synchronized with the server
Unique secret key
IMEI number of user's mobile phone
Hash salt based on the domain name of the target website

The application for generating OTP can be provided on the user's mobile token in a number of ways including Bluetooth connection, WAP Push, downloading, SMS request from a short-code or a long number or an URL from mobile Internet portal or from any relevant applications store.

This scheme also protects against phishing attack by using a hash salt based on the domain name of the target website. If the user enter password at an imitated website of attacker, that site's domain will be used as the hash salt. This will produce totally different OTP than the original one.

C. Third Factor (Optional)

If user opts for this factor to be included in his password then the possible options to form this factor are user's PIN or he can select to enter text password. Another option is to answer the selected questions from list provided.

D. Password Space Size

Introducing graphical environment instead of blank textual password increases the usability of the proposed scheme. But equally important is the security of the authentication scheme. Size of the password space is the major factor affecting security of any authentication system. The proposed systems claim to provide a superior space of possible password combinations compared to traditional 8-character textual passwords.

Password space size for proposed scheme is dependent on number of categories (c), number of objects available as option (ob) and all the possible combinations of them. More the number of categories i.e. type of interactions in the virtual environment; more will be size of password space.

$$S = \sum_{i=1}^{n} Pc(j)_1 \, Pob_1$$

j>=1 & j<=m, m is no. of categories, n is total no. of interactions chosen by user. P is the permutation function.

E. Password Recovery

Many of the websites visited by the user where he had created the account are rarely revisited. This is the reason password recovery systems are equally used as much the login procedures. Therefore, password recovery and login system are the two entrances for attacker to gain privileged access to legitimate user's account in order to break confidentiality and integrity. If either of the two has design loophole then that will open the second entrance for the attacker. Recently many websites have implemented strong authentication system using latest techniques but the recovery system is still following the traditional method of presenting security hint questions to the user which has quite predictable answers.

In the proposed scheme, the recovery system has four categories from which user need to select one. For the chosen category, user has to face four questions out of which he may select two or three questions. For selected questions he has to provide answers. This process is performed at the time of registration. Later if the user wants to recover his password, he must select the same category and set of questions. Based on their answers some hint is sent to the user mobile. User has to enter the data according to the hint and he gets back his password.

IV. CONCLUSION

This paper has proposed a new multifactor authentication system based on graphical password. This approach is highly secured and can be used by layman. It is a web authentication mechanism for public and un-trusted network. Presented method doesn't need a familiarization or a lengthy password setup process. It employs a cell phone as the second factor of authentication in conjunction with graphical password. This system has the advantage that the authentication task is more reliable, easier and fun to use. Being purely recognition based system, it reduces user's cognitive load helping users to stop reusing password for multiple web accounts; specially on low as well as high security sites i.e. sites with varying security levels, avoiding cross site account compromise attack. Since user's cognitive load is reduced, they will not copy down password for memorizing it. This avoids leaking of password. Even if they want to copy it, they can't write password as it is since it's not a string. What user knows is a set of actions. Only they can write the hint for generating password. But such hint may not be completely useful for the attacker. It helps user to choose non-trivial but difficult to guess password. Lastly, it is resistant to the attacks like phishing, MITM, Malware and Shoulder Surfing attack apart from tradition brute force attack.

ACKNOWLEDGEMENT

The author would like to thank BCUD, University of Pune for funding Research Project Grant and the involving research which forms the base for this paper.

REFERENCES

[1] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[2] www.passfaces.com.

[3] http://myuceel.etu.edu.tr/gpex/.

[4] Kemal Bicakci, Mustafa Yuceel, Burak Erdeniz, Hakan Gurbaslar, Nart Bedin Atalay, "Graphical Passwords as Browser Extension: Implementation and Usability Study", IFIP Advances in Information and Communication Technology Volume 300, 2009, pp 15-29.

[5] Passlogix V-GO, "www.passlogix.com".

[6] www.confidenttechnologies.com Confident ImageShield, Image-Based Authentication For Websites.

[7] "WHEN PASSWORDS AREN'T ENOUGH", White Paper Published By: Confident Technologies, Mar 16, 2011.

[8] Alireza Pirayesh Sabzevar, Angelos Stavrou,"Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS) ISBN: 978-0-7695-3493-0 2008.

AUTHORS

First Author – Ms. Aruna K. Gupta, M. Tech. (CSE), JSCOE, Pune, aruna_gupta@rediffmail.com