Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A More Secure Authentication through a Simple Virtual Environment

Dasika Ratna Deepthi*
Professor in Dept. of CSE, SNIST
Yamnampet, Ghatkesar
Hyderabad, India
E-mail: radeep07@gmail.com

T.Sujanavan
Dept. of CSE, SNIST
Yamnampet, Ghatkesar
Hyderabad, India
E-mail: tsujanavan@gmail.com

Abstract: we propose an authentication system with a simple virtual environment which could address some of the open authentication issues of the industries. In this system, user interacts with the virtual environment and the sequence of interactions are gathered by a background process (the proposed authentication system) which decides whether the user is authenticated user or a hacker, depending on which the system allows or denies the access to resources. Many existing authentication schemes are based on a single factor mechanism and due to their backdrops, found to be unsuccessful. Examples of such systems are authentication systems with textual passwords, biometrics, graphical passwords etc. Even though, research is around such failures of the systems, still notorious attacks on the systems continue. And hence, we propose an authentication system with a simple virtual environment which is more secure and simple to use to solve some authentication issues.

Keywords: Authentication system; virtual environment; textual passwords; biometrics; graphical passwords.

I. INTRODUCTION

Compared to the past decades, at present there is a rapid increase in the use of internet and the computer systems through which large amount data is handled, demanding the need of secure authentication systems. There are different variants of users starting with the simple household users to the large business/industry customers. Everyone has some sought of information to be securely stored which are not to be stolen, edited or viewed by somebody else. The information stored online could range from a small text file to that of a huge footage video. Though here, we are not concerned with the file size, the organizations that are providing online storage to users do have threats from all sorts of notorious criminals [1]. The main entrance to the unauthorized access is the authentication system.

Many people have brought revolution over the internet for its security [2] [3], still, the number of criminal minds have also been increased [4]. Earlier, we used to utilize a textual secret e.g. password, later people thought of that the password could be estimated. Hence, they came up with the idea of smart cards e.g. RF-ID, even though, these cards could be stolen [5]. Most of the users were not satisfied with such systems because they involved a process of recall where users have to reproduce a secret every time when they need to access their data, which gave raise to the invention of the recognition methods, as an alternative of the recall, examples, graphical passwords (of some type) & biometrics [6] [7] [8].

Human do possess lack of memory to reproduce a textual password after a long time of non-utilization of an account could lead to misery. But in recognition mechanism (used in the graphical password scenario) the system shows the users a set of graphical passwords out of which the user previously elected one, provides a login. Thus, in this scenario we overcome the fact of memory loss.

The graphical password also did include some kind of recall, which the biometrics had overcome. Biometrics proven to be a more secure method of access, but at the same time, gave trouble in identifying the attributes of the legitimate user. E.g. In fingerprint recognition if the user's finger had a cut or involved a foreign material as an obstruction then, the biometrics system would not recognize the user. Though the biometrics was already available with the user physical aspects it did also possess disadvantages based on several factors such as consistency, uniqueness, and acceptability.

Hence, in such a situation simply constructing a system blindly based on a single factor could involve vulnerability. In this paper, we propose a method that utilizes all the mechanisms above with a virtual environment. However, many researchers have tried to bring such mechanisms [6] [7] [8] [9]. We construct an optimal mechanism of utilizing different schemes with reduced overhead to the network and with the more user friendly interactions.

The proposed system depicts a virtual environment with some items placed randomly in it. The user's password consists of a sequence of interactions with the items in the environment [10]. These actions performed, indirectly describe the user's physical and mental behaviors to the authentication system. The authentication system consists of a background process that utilizes an algorithm proposed in this paper to identify the legitimate user.

As the method doesn't only depend on the mental behavior but also on the physical characteristics of the user, hence, it is safe, secure and easy to use.

The remainder of this paper is organized as follows: Section II discusses related inventions and innovations. Section III introduces the proposed scheme in which we also discuss the guidelines of building the virtual environment and its possible applications. In Section IV we elaborate on security analysis including possible attacks and countermeasures. Section V presents the experimental conditions. Finally, in Section VI, we conclude and confer the future work.

II. RELATED INVENTIONS AND INNOVATIONS

Graphical passwords which were introduced by Blonder brought a new revolution in authentication systems [11] [12] [13]. It consists of both recall and recognition methodologies e.g. Pass-faces, pass-point, DAS etc. Though, the graphical passwords could produce a longer password size it suffered from the shoulder surfing attack.

The pass-faces is a recognition type of method which consists of selecting an image by a user from a set of images projected on the screen. For this authentication system to work, initially the users need to specify a set of graphical images of his choice to the authentication system through a secure channel.

The pass-point method is a recall method where the user needs to select different points on a picture that resembles his password [14]. The DAS (Draw a sketch) method also falls in this category where the user needs to draw his login sketch on a grid (5x5, 10x10 or 25x25). The login involves in identifying the lines that pass through the different grids present on the screen.

Biometrics authentication system even though became popular with a short start, still, people are afraid of using it as it involves in recording the user's physical aspects posing a threat to his privacy. In addition, some users resist the idea of a low intensity infrared light or any other kind of light directed to their eyes, such as in retina recognition systems. Moreover, biometrics cannot be revoked, which leads to a dilemma in case the user's data have been forged. Unlike other authentication schemes where the user can alter his password at times of threat to privacy [15] [16], a user's biometrics cannot be revoked.

Many authentication systems are based on tangible objects and are referred to as token-based systems. Many token-based systems are vulnerable to theft and loss [1] [5]; therefore, most token-based systems require a personal identification number followed by a textual password for authentication e.g. a debit or a credit card.

Our schema involves the efficient utilization of all the mechanisms discussed above and it is small in size and an optimal solution.

III. THE PROPOSED SCHEME

This scheme is proposed keeping in mind the requirement to overcome the disadvantages of all the previous schemes and is outlined as follows:

1. The system should be smaller in size. As the utilization of the users on the internet is higher, the requirement of the scheme also increases.
2. The newly proposed scheme should be easy to use.
3. It should produce a higher password size compared to the previous schemes.
4. Password provided by the scheme should be easy to remember.
5. It should consist of passwords that are not easy to be written down.
6. Users should have the freedom of selecting their passwords [14].
7. The newly proposed system should provide a method for changing passwords.

Hence, keeping in mind all the above requirements the proposed system was designed.

A. The proposed system

The system consists of merging different authentication schemes together. The system presents a simple virtual environment containing various items. The user goes through this environment and changes the state of the items [10]. The system simply combines the sequence of user interactions that occur in the virtual environment which is depicted in Fig. 1.

The system can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a virtual environment that contains items that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified.

For example, the user can change the state of a window or a door in the virtual environment by simply clicking over it, later switch on a light bulb and finally click on login. The combination and the sequence of the previous actions construct the user's password (action sequence recorded by a background invisible process as in Fig. 1). Items can be any object that we encounter in real life. Any obvious state changes and interactions toward the real-life objects can be done in the virtual environment toward the items which may include:

1. Opening/closing windows or doors.
2. Typing a textual password on a virtual keyboard.
3. Switching on/off the lights.
4. Performing biometrics by selecting a virtual item in the environment.
5. Identifying a graphical password.
6. Providing a token for identification e.g. RF-ID on selecting an item.
7. Writing on a paper present in the virtual environment.
8. Moving an item.
9. Any other authentication scheme which is to be developed in the future.

The state change performed on an item differs from that of a different item hence, preserving the unique changes made at an item for later recognition process of the authentication system. Therefore, to generate the legitimate password, the user must follow the same scenario performed by him initially. This means changing state of the same items and performing the exact actions in a proper sequence.

B. Password selection and inputs

Even though many items in the virtual environment are present additionally (passive components) could mean nothing to the user. For example, user clicks on the roof and clicks on the floor. But, such kind of inputs that do not generate any action could be utilized for confusing the fake cameras or tracker objects installed.

The virtual environment consists of many kinds of actions and the range of the states for a single object could range from small to big. For example, user's password could consist of a simple activation of a light bulb or as complex as solving a riddle.

The above procedure is easy to perform and changeable. It looks simple but it also involves complex calculations to convert the selections and inputs to match the user's behavior by the authentication system. Though user has the freedom of selecting the items to be projected, the item properties or attributes are never revealed by the system to the user

therefore, we can say that protecting the privacy of the authentication system is the methodology, involved here.

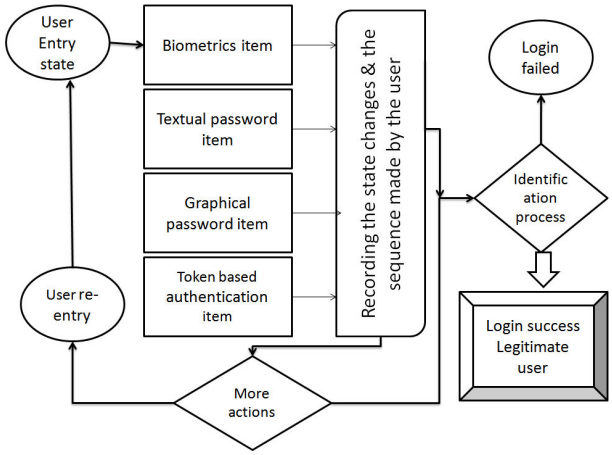

Figure 1. Representation of the flow of the authentication system

As we mentioned previously that a virtual environment could contain anything, but the developer should keep in mind the following factors:

1. Size of the environment – to decrease the overhead, the size of the environment should be lower in size. If the designer needs to use a large environment then he should use compression algorithms to reduce the size of the images or else it tends to overload the network bandwidth.
2. Number of items – the developer should not project a large number of items to be displayed, which could confuse the user. Limiting the number of items helps the user to understand the items.
3. Uniqueness of the items – the developer should construct the environment in such a way that the user uniquely identifies the items. For example, there should not be two different items that solve the same purpose.
4. Importance of the environment – the environment is constructed to deploy the authentication system and this should be kept in mind of the developer and should not develop an inappropriate environment. For example, involving alien objects, distracting objects etc.,

C. *Applications of the system*

As the system, we propose, is of small size & it is having the higher safety which could be implemented every where, details given below.

1. Over the Internet – at the login page for emails, social networking sites & blogging.
2. Cash dispense machines – at ATMs and credit card machines.
3. E-business web-sites – as the revolutionary growth of e-commerce requires safe authentication at rapid speeds.
4. Personal devices – protecting personal data on desktop PCs, Laptops & smart-phones.
5. Home security – at door locks and garage shutters.
6. Research facilities – protecting secret data e.g. information at robotics, nuclear & defense laboratories.
7. Industries & corporate business – avoiding theft of objects or data e.g. blue-prints, data on web-servers etc…

IV. SECURITY ANALYSIS

In order to analyze how tough is a security algorithm, the best way is to crack it, open without knowing the password. Even though the proposed system looks simple, it is very hard to knock it down as it results in equally cracking down all the security programs possessed by the system. Still the hacker needs a huge amount of knowledge and data to gain that is impossible, as the state and attributes of the items are kept hidden even to the legitimate user and sequence is hidden from the administrator/working staff at the security company. There are also some organizations that provide a validation process for the authentication systems [17].

Still referring back to the standard principles of estimating the crack time by just looking at the password size even then, as the size of the password generated is huge compared to other algorithms, it makes impossible to be cracked.

The password size of the proposed system could be explained as follows-

Consider,

PS(max) = maximum password size
S(i)= selections made over an item ‘ i’
SC(i)= item ‘ i’ state changes undergone

Then, the total number of passwords that could be generated can be calculated using the following formula

$$\prod(PS(max)) = \sum_{n=1}^{n=PS(max)} (S(i))^n \cdot \sum_{n=1}^{n=PS(max)} (SC(i))^n$$

When, the above is compared to the rest of the algorithms, it could be observed that though the length of the password is small, the size of the password is very huge.

V. EXPERIMENTAL CONDITIONS

In our experiment to have a decrease in code size, we have used JSP (Java Server Pages) which is also available on every system nowadays as a third party application hence, helps in an easy deployment. We did not use any kind of graphic card or acceleration devices in designing the virtual environment. The training for building the virtual environment was taken from virtual home construction software [18].

The Apache Tomcat software processes the server requests from the client and as the software is also available as a mobile version [19], an immediate backup could be available at the time of breakdown.

Basically, the environment was setup only based on the graphical & textual passwords. Biometrics or any other new authentication system could also be attached as a module, easily, by introducing a new interaction item in the virtual environment.

VI. CONCLUSION & FUTURE WORK

Until now many authentication schemes only utilized the user's physical or mental behavioral attributes and always were single factor dependent. There are also schemes based on a token, which are feared of theft or loss. But this algorithm solves the authentication issue by utilizing all the schemes put together.

However, as mentioned before, all authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

The present system solves all the issues related to the past algorithms by efficiently utilizing them, keeping in mind their disadvantages [1] [5] [14] [15] [16] [20] hence, building a user friendly, safe, secure and easy to use authentication system that could be applied to all fields.

The scheme mentioned by us is in its developing stages and hence also has a drawback of shoulder surfing attacks. A keen observation of the login procedure by the hacker could reveal the password therefore we suggest that the approach is performed in a secure environment were no trackers or tracking devices are present.

The above disadvantage could be a matter of future work, involving a research in overcoming the attack that could be an enhancement of this paper.

VII. REFERENCES

[1] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.

[2] Pilot authentication system – Mark E.Nikolsky – U.S. Patents–April10,2003 - http://www.freepatentsonline.com/y2003/0068044.html

[3] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.

[4] Shopping Scams - CBS News - Nov 16, 2010

[5] ATM fraud- Banking on your money - Dateline NBC - Consumer Alert - http://www.msnbc.com

[6] Regunathan Radhakrishnan, Nasir Memon - On The Security Of The Sari Image Authentication System – 2002 - Polytechnic University, Brooklyn.

[7] Norman Fraser Ph.D. - The usability of picture passwords - Chief Executive, Tricerion Group

[8] Ankesh Khandelwal, Shashank Singh, Niraj Satnalika - User Authentication by Secured Graphical Password Implementation - 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 25

[9] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th USENIX Security Symp., San Diego, CA, Aug. 2004, pp. 1–14.

[10] Somayeh Dodge - Evaluating different approaches of spatial database management for moving objects – "http:///www.GISdevelopment.net" ---> Technology ---> Geographic Information System

[11] What is 3D Password Scheme – http://www.technospot.net

[12] FABIAN MONROSE AND MICHAEL K. REITER - Graphical Passwords - ch09.10346 Page 161 Friday, August 5, 2005

[13] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472.

[14] Anne Adams and Martina Angela Sasse - USERS ARE NOT THE ENEMY. Why users compromise computer security mechanisms and how to take remedial measures. - December 1999/Vol. 42, No. 12 COMMUNICATIONS OF THE ACM

[15] Your face is not your password- Duc Nguyen – BKIS, Vietnam – http://www.bkav.com.vn

[16] How to make the fakefingerprints (VIRDI) – http://www.shareshare.com

[17] Office of Information Collection: The Exchange Network E-Authentication Pilot - Credential validation services - December 2005

[18] 3D Home Architect developed by Brøderbund in the 1990s - http://www.3dhaonline.com/

[19] RACCOON (the mobile apache tomcat) - http://sourceforge.net/projects/raccoon/

[20] Jinhai Wu1, Bin B. Zhu2, Shipeng Li2, Fuzong Lin - New Attacks on Sari Image Authentication System - State Key Lab of Intelligent Technology and Systems, Beijing, Microsoft Research Asia.

