3D-WEBAUTHEN: HIGH DEGREE OF AUTHENTICATION FOR WEB APPLICATION DEVELOPMENT

Waraporn Viyanon
Computer Science Program, Department of Mathematics
Faculty of Science, Srinakharinwirot University
Bangkok, Thailand
waraporn@swu.ac.th

ABSTRACT

Nowadays accessing information typically is performed via web based applications because of the convenience, ease, and speed of the Internet. However there is a lack of security in terms of authentication because most web applications use easily circumvented textual passwords to identify a user. The purpose of this paper is to present a method of authentication with Multi Password Schemes in 3D environment for web applications called 3D-WebAuthen providing better security than textual passwords. The prototype of authentication powered is developed by HTML5 and WebGL. The passwords are created using PassPoints, Draw-A-Secret (DAS), and textual password techniques and encrypted before storing them. The results of our experiment show that the prototype can be run on Mozilla FireFox and Chrome, the password space increases compared to that of traditional textual passwords. The system is evaluated using SQL Injection method to test its security and it passes all tests. According to the result of the study with this system carried out users, we found that the users can easily use the authentication system and are satisfied with this approach.

Keyword: Three Dimensional Passwords, Authentication, Password Security

INTRODUCTION

Web applications are client–server applications in which a web browser provides the user interface. They are a critical part of our daily lives, used for banking and financial management, email, online shopping and auctions, social networking, and much more. The security of information manipulated by these systems is crucial, and yet these systems are not being implemented with adequate security assurance. The convenient way to protect these systems from intruders is authentication with passwords.

Passwords are the predominant form of authentication system used by today’s websites. Textual passwords remain the most common choice because they are easy and inexpensive to implement, are familiar to all users, allow users to authenticate themselves without requiring privacy things such as biometrics and physical tokens.

Graphical password schemes (Biddle, Chiasson, & Van Oorschot, 2012) have been proposed as an alternative to textual passwords in applications that support graphics and mouse entry. These schemes require users to remember pictured-based information instead of text, motivated in part by the fact that humans have a remarkable capability to remember pictures. One disadvantage to most graphical password schemes is their
susceptibility to shoulder-surfing: attackers may observe or record users as they enter passwords and subsequently log in with the observed credentials.

The greatest weakness in the use of passwords is that users tend to pick short passwords that are easy to remember and thereby have very low entropy and are easy to guess or broken by dictionary attack. Another weakness is the ease of third party eavesdropping. Passwords typed at a keypad are easily observed or especially in areas where attackers could plant wireless cameras or hardware keystroke sniffers. Key loggers capture keystrokes and store them somewhere in the machine, or send them back to the adversary. Shoulder surfing is a well-known method of stealing other’s passwords and other sensitive personal information by looking over victims’ shoulders while they are sitting in front of terminals or in front of an ATM machine (Alsulaiman & Saddik, 2006).

Passwords can be a combination of many factors such as combination of a textual password and a graphical password. In general, the more factors that are used in the authentication process, the more robust the security process will be. When two or more factors are used, the process is known generically as multi-factor authentication.

3D passwords (Alsulaiman & Saddik, 2006) combine existing authentication schemes into one three-dimensional virtual environment. The three-dimensional virtual environment consists of many objects. Each object has different responses to actions. The user’s 3D password is created by the combination of actions, interactions and inputs toward the object in the 3D environment. The 3D password has a large number of possible passwords because of the high number of possible actions and interactions towards objects.

This paper presents a method of authentication with combination of multi password schemes in 3D environment for web applications called 3D-WebAuthen. The prototype of authentication is powered by HTML5 and WebGL. The prototype can be run on average computer machines (Processor: core i3, core i5, or core i7 Ram: 2GB, 4GB, 8GB Hard Disk: 500GB, 1TB, or more VGA: 1GB, 1.5GB, 2GB) via web browsers.

RELATED THEORIES AND TECHNIQUES

Password Space

Password space is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. It estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability (McDowell, Rafail, & Hernan, 2004). It is usual to specify password space in terms of password entropy, measured in bits, a concept from information theory. Instead of the number of guesses needed to find the password with certainty, the base-2 logarithm of that number is given, which is the number of "entropy bits" in a password. (Burr, Dodson, & Polk, 2006). Password entropy is an easy way to identify how hard the password is to guess.

Graphical Password Techniques

Graphical password is a technique that uses images as passwords. The concept of graphical password is first proposed by Blonder in 1996 (Blonder, 1996). His approach was to let the user click, with a mouse or stylus, on a few chosen regions in an image that
appeared on the screen. If the correct regions were clicked in, the user was authenticated, otherwise the user was rejected.

Draw-A-Secret (DAS) (Jermyn, Mayer, Monrose, Reiter, & Rubin, 1999) is a graphical password scheme replacing alphanumeric password strings with a picture drawn on a grid. This method allows users to use a set of gestures drawn on a grid to authenticate. The user's drawing is mapped to a grid on which the order of coordinate pairs used to draw the password. The passwords are recorded in a sequence as shown in Figure 1. New coordinates are inserted to the recorded "password" sequence when the user ends one stroke (the motion of pressing down on the screen or mouse to begin drawing followed by taking the stylus or mouse off to create a line or shape) and begins another on the grid.

A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Users may choose any place in the image as a click point. After a sequence of click points (i.e., pixels) is chosen (a "password"), the system encrypts the password and calculates a tolerance region around the chosen pixels. When logging in, to make a valid click the user will have to click within this tolerance. The size of this tolerance can be varied, but it should not larger than 5x5mm and smaller than 10x10 pixels. Figure 2 shows the password created by PassPoints techniques. The sequence of points is defined as the numbers.

3D Passwords

3D password is a multifactor authentication scheme that combines various authentication schemes into a single 3D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object (Alsulaiman & Saddik, 2006).

It is the user’s choice to select which type of authentication techniques will be part of their 3D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3D password and given the large number of objects and items in the environment, the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user’s 3-D password. Therefore, the resulted password space becomes very large compared to any existing authentication schemes.
HTML5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. Its core aims have been to improve the language with support for the latest multimedia while keeping it easily readable by humans and consistently understood by computers and devices (web browsers, parsers, etc (Van Kesteren & Pieters, 2008).

WebGL

WebGL (DeLillo, 2010) enables web developers to embed rich 3D content into webpages, which can be rendered without using proprietary plugins. JavaScript, on the other hand, allows for interaction between the 3D content and the HTML UI of the webpage. At the beginning of 2011, two major browsers, Firefox and Google Chrome, already support WebGL by default and make 3D graphics available to a broad range of end-users.

GLGE

GLGE (GLGE: WebGL) is a JavaScript library that was made to ease the use of WebGL. The basic intention of GLGE is to mask WebGL from the web developer (GLGE.org). This allows for an easy way to creates 2D and 3D graphics without worrying about lower level things. When using regular WebGL, shaders have to be written to deal with the lower level drawing of vertices and pixels. GLGE does this for the programmer. The programmer only needs to either define the scene, which contains objects, a camera, and lights, either within an XML file (which is usually the case) or directly in the JavaScript. Within an xml, the programmer can use tags to create different aspects of their scene. In the HTML file which contains the programmers’ JavaScript code, the programmer must create a new GLGE object and load the XML file. This takes all the low level shader programming away making for an easier WebGL experience.
OVERVIEW OF 3D-WEBAUTHEN

In traditional web applications during creation of user accounts, the users are asked for their password and some security questions after that the information is stored in a database. This approach is vulnerable to SQL injection attacks (Halfond, Viegas, & Orso, 2006). 3D password scheme can overcome this problem.

3D-WebAuthen is proposed to be an authentication prototype for web applications requiring high security. There are two groups of people using this system which are the administrator/developer and end users as shown in Figure 3. The administrator or developer is responsible for designing 3D environment and managing user account. The end users need to create their password in order to access the system. This prototype allows users to change their password, in case they forgot the password. The users are permitted to access the system if they put the correct 3D passwords which are the sequence of their actions recorded during the registration.

The system is required to have 3D environment development in order to let users provide their 3D password. The 3D environment is designed using Google Sketchup (Trimble Navigation) and Blender as shown in Figure 4(a). The registration and authentications pages are created using HTML5 and GLGE (WordPress) which defines a camera, objects, and lights in the 3D environment. In Figure 4(b) when a user registers to the system, his password is stored as a string of a sequence of his actions which can be a combination of textual, PassPoints, Unlock pattern passwords. Before the password is stored in the database, it is encrypted with MD5 algorithm (Rivest, 1992). When the user wants to access the system, it is required that he has to do exactly the same sequence of his actions. The string of the sequence of the user’s actions is encrypted with the same algorithm. The password is verified by matching the encrypted string from authentication page with the retrieved password from the database. If they match, the user is allowed to access the system.
The details of the system are categorized into three steps: (1) 3D Environment creation, (2) user registration, and (3) users’ authentication.

**3D Environment Creation**

To create a 3D environment, there are three steps which are (1) designing the 3D objects such as a computer, frame of a picture, TV, refrigerator, lamp, etc, (2) placing the objects in the scene which is like a room, and (3) defining authentication scheme for each object. It is not necessary that all objects embed an authentication scheme.

All the 3D Objects presented in Table 1 are created using Google sketchup which is a free 3D modeling program (Trimble Navigation). The objects are exported in collada format (or .dae extension) in order to interchange information with 3D applications or 3D library.

The 3D environment is created by defining a scene, which contains the objects, a camera, and light using Blender (Blender Foundation, 1995), which is a free and open-source 3D computer graphics software product. The scene is exported in XML format as shown in Figure 5. This is the most common way to setup GLGE materials. Figure 3 shows the structure of the exported XML file.

The registration and login pages contain the 3D scene created in the previous step using the help of HTML5, MySQL, PHP, and JQuery. The 3D environment is embedded by HTML canvas element as shown in Figure 6. The registration and login pages are displayed in Figures 7 and 8.

**Users’ registration**

The registration procedure consists of four steps via 4 pages:
1) Instruction page
This page provides the information of how to register to 3D-WebAuthen.

2) Personal information page
   This page allows users to provide their information such as firstname, lastname, email, and username.

3) Creating 3D password page
   This page let users explore in the 3D environment and decide which objects they would like to store their password. The system forces the users to have a combination of passwords such as a textual password and PassPoints.

4) Re-creating 3D password page
   This page is to confirm the users’ password.

TABLE 1 3D Objects, Password schemes, and Interactions in 3D-WebAuthen

<table>
<thead>
<tr>
<th>3D Object</th>
<th>Password scheme</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Desktop</td>
<td>Textual password</td>
<td><img src="image" alt="Textual Password Interaction" /></td>
</tr>
<tr>
<td>Picture</td>
<td>PassPoints</td>
<td><img src="image" alt="PassPoints Interaction" /></td>
</tr>
<tr>
<td>Television</td>
<td>PassPoints</td>
<td><img src="image" alt="PassPoints Interaction" /></td>
</tr>
<tr>
<td>Refrigerator</td>
<td>DAS: Pattern Unlock</td>
<td><img src="image" alt="DAS: Pattern Unlock Interaction" /></td>
</tr>
</tbody>
</table>
After a user confirms his 3D password, the password will be stored in a database. It is a string that contains a sequence of actions. For example, if the user do the following actions.

1. Click the computer desktop, enter a textual password such as “qaz”.
2. Click the refrigerator, draw a pattern of password such as cells(2,2) (3,2) (3,3) (2,3) (2,2) (2,1) respectively.
3. Click the picture, point two positions of the picture such as coordinate (1,3).

The string [com]qaz[fridge]2_2,3_2,3_3,2_3,2_2,2_1[pic]1_3 represents the password. The square brackets identify which object has been clicked. The characters not in the brackets represent the password depending on its password scheme. This string is
encrypted and calculated for a tolerance region around the chosen pixels before storing in the database.

**Users’ sign-in**

The sign-in process

1) First, the user will be asked for his username like regular authentications.
2) The user explores in the 3D environment and interacts with the objects that are related to his password in the right order.
3) The action sequence is converted to be a string as explained in the previous section and encrypted. The encrypted password is compared to the password stored in the database. If they are a match, the user is allowed to access the application, otherwise go back to the authentication page.

![Figure 7](image1.png) Registration page of 3D-WebAuthen

![Figure 8](image2.png) Sign-in page

**AN EMPIRICAL STUDY**

**Supported web browsers**

3D-WebAuthen is required to run on a web browser. It was tested with web browsers for desktop platform. These included Google Chrome, Mozilla Firefox, Internet Explorer, and Opera. A testing matrix was developed to evaluate HTML5 and WebGL
support, graphics benchmark. For graphics benchmark, Fishtank (Internet Explorer Test Drive) and Solar system (Regis) were selected to be the test driver. The result of the test is shown in Table 2

TABLE 2 Browser Testing for 3D

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Google Chrome Version 24</th>
<th>Internet Explorer Version 9</th>
<th>Mozilla Firefox Version 18</th>
<th>Opera Version 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML 5 support:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canvas</td>
<td>Support</td>
<td>Support</td>
<td>Support</td>
<td>support</td>
</tr>
<tr>
<td>WebGL: GLGE</td>
<td>Support</td>
<td>Not support</td>
<td>Not support</td>
<td>Support</td>
</tr>
<tr>
<td>Graphics benchmark:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FishIE Tank</td>
<td>FPS 60 FPS</td>
<td>60 FPS</td>
<td>60 FPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory 378.3 MB</td>
<td>299.8 MB</td>
<td>299.8 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPS 100 FPS</td>
<td>97 FPS</td>
<td>97 FPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory 240.9 MB</td>
<td>200.1 MB</td>
<td>200.1 MB</td>
<td></td>
</tr>
<tr>
<td>Chrome Experiments WebGL Solar System</td>
<td>2000 fish</td>
<td>FPS 71 FPS</td>
<td>59 FPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory 246.0 MB</td>
<td>195.9 MB</td>
<td>195.9 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPS 41 FPS</td>
<td>36 FPS</td>
<td>36 FPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory 247.9 MB</td>
<td>196.3 MB</td>
<td>196.3 MB</td>
<td></td>
</tr>
</tbody>
</table>

Password space

The information content of a password space defined in (Jermyn, Mayer, Monrose, Reiter, & Rubin, 1999) as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose". It is a measure that determines how hard the attack is.

3D-WebAuthen combines three different password schemes which are textual password, PassPoints, and DAS with four different 3D objects. Figure 9 shows password entropy of 3D-WebAuthen compared with other password schemes.
Since 3D-WebAuthen is a multifactor password, it makes sense that entropy password of this approach is stronger than the compared password schemes.

**SQL Injection Test**

SQL injection attack (SQLIA) is considered one of the top 10 web application vulnerabilities of 2007 and 2010 by the Open Web Application Security Project. SQL Injection may be a concern for system administrators. From the experiment using SQL Inject Me (Security Compass), the system’s authentication page passed all the tests (29,240 tests) as shown in Figure 10.

![Figure 10 The test results from SQL Inject Me](image)

**Satisfaction evaluation**

3D-WebAuthen was tested with 10 users to evaluate their satisfaction with user satisfaction survey.

After letting the users use the system, they completed a user satisfaction form. This survey covers three main aspects:

![Figure 9 Password Entropy of each password scheme](image)
• Information on users’ background of using different authentication schemes.
• Satisfaction on using the registration page, changing password
• Tendency of using the system in the future.

Characteristics of Respondents

70% of all respondents were familiar with textual password. The users concern that textual password is not safe enough, with 60% of all respondents. 50% of the users know what the Pattern Unlock is.

Users’ usability satisfaction

The respondents rated each item on a 1-5 scale by their satisfaction on usability. 1 means not satisfied at all or very low. 5 means very satisfied and very high. The result of the survey is show in Figure 11.

![Usability & Satisfaction](image)

Figure 11 Users’ usability satisfaction

70% of the respondents chose to have 2 objects to be their passwords. The rest picked 3 objects as their passwords. Some respondents took some time to learn how to create their 3D password. Most respondents preferred to have graphical password rather than textual password.

Tendency of using the system

Most respondents preferred to use the 3D password like this prototype as authentication because it provided more security for web application and it didn’t require any extra token or user’s personal information. 78% of respondents would like to have 3D password for critical web applications such as internet banking.

CONCLUSION

3D-WebAuthen is the authentication prototype consisting of registration to the system in order to create a 3D password, which is a sequence of action, authentication with the password. 3D-WebAuthen has strong password since it combines many factors such as textual password, PassPoints, and DAS to create passwords. The experiment shows that the password space increases compared to textual passwords and PassPoints. This system passed all the SQL injection tests. From the satisfaction survey, the users are satisfied with the system and confident to use it since it does not require privacy things and physical tokens.
However the system can be run on Chrome and FireFox. This may be an obstacle for the system to be used in the future. Also, HTML5 is in initial state. Some browsers may display 3D environment differently. Hopefully, in the near future, this problem will be solved.

REFERENCES