Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.5, No.11, 2015

3D Shapes Technique to Improve Mail Services Authentication

Mr. Mohammed Hussain Ali , Lecturer Mrs. Tamara Saad Mohamed , Lecturer
Cihan University \Sulaimaniah \Iraq

Abstract
In today's world, security is important aspect in day to day life .So, everyone used various ways for security purpose. users use passwords for their mail security and Generally, everyone uses textual password. Textual password is combination of alphabets, characters and numbers. users keep textual password as name of their favorite things, actors or actress, dish and meaningful word from dictionary. But the person who is very close to that person can easily guess the password. Graphical password is advanced version of password. Graphical passwords have received considerable attention lately as Potential alternatives to text-based passwords .Graphical password is composed of images, parts of images, or sketches. These passwords are very easy to use and remember.To Drawbacks of previously existing authentication techniques. We present A new improved authentication technique ,The proposed system is about a new technique to generate password ; there are three password fields each field is about one character and one number, when the user fill the three fields the system security generate a special algorithm which is available in the user's machine itself to convert the content of the three password's fields to a 3D graphical shape which are saved and transfer in the form of 3D shape in server side . so all the password have been stored in the form of 3D shape at the server . so anybody want to hack password he will face difficulty to guess the exact password because he can see only the shape not real password (the three pairs of characters and numbers) .
Keywords : Authentication , 3D Shape , Processing 2.0 mode P3D technique .

1.Introduction

Authentication technology allows the receiver of an email and the Internet Service Provider (ISP) to confirm the identity of the sender. If the identity of the sender can not be authenticated, then ISPs may reject the message, or put it through additional filters to determine if it should be delivered. Without authentication, your chances of being filtered by major ISPs are greatly increased and the chances of them blocking spoofed messages impossible .Email authentication is important because it addresses one of the fundamental security problems inherent to email sending technology. By exploiting such weaknesses phishers and spoofers have been able to thrive. Authentication is integral to preventing phishing and other fraud while playing a key role in the emerging reputation and accreditation systems that will drive the future of email. As a legitimate business, authentication is not optional; rather it is essential to securing your brand and online reputation.
Ideally there are two different types of Authentication schemes are available according to nature of scheme & techniques used, those types are:

1.1 Recall based

In this authentication tech. user need to recall or remember his/her password which is created before . Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

1.2 Recognition based

In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used.

Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time.To improved the authentication of mailing services we will present this idea , to create a new software which is carry a special authentication technique to be installed and setup to the subscriber computer or any machine he/she want to use , so that piece of software should available at the e-mail account provider .

2. Authentication

The process of identifying an individual usually based on a user name and password. In security systems, authentication is distinct from *authorization ,* which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he \ she claims to be, but says nothing about the access rights of the individual.

3. Drawbacks In Existing Authentication System

3.1 Textual Password

Textual Passwords should be easy to remember at the same time hard to guess. But if a textual password is hard to guess then it is very difficult to remember also. Full password space for 8 characters consisting of both numbers and characters is 2 *1014.From are search 25% of the passwords out of 15,000 users can guessed correctly by using brute force dictionary.

4. Proposed system

To improve the authentication system of the mail services we present this technique which is deal with three password's fields instead of one , each one allowed for only one content's character and one number to produce a 3D shape which is saved in the database server and transfer through system by using a special piece of software ,This piece of software can established by converting each field contents (character and number) to one point (one axes) then we will collect three points (three axes) to produce a 3D shape .to produce a 3D shape we have to use for example Processing version 2.0+ P3D algorithm , this algorithm used to generate a 3D shapes from the three passwords(three points) the user have to entered . these piece of software should be provide by the company of the mail provider . so the suggestion is : that is when the user want to create account's mail for example want to create a yahoo mail the first step before entering user name and the three field's passwords to accepting information from the user is to generate a piece of software from yahoo mail provider to the user machine and ask the user to instill and setup that software . second step is the user will asked to enter the user name , passwords and to fill other information .because of all above processing is done in the user's machine we will avoid a lots of attacker's passwords , so some types of them can see only the 3D shapes can not exam the real passwords , and even the knowing those shapes not useful because when the attacker want to send that shape to the provider to get access to the user account , the provider can not accept that shape because the provider want to check the source of the sender by checking that piece of software which is installed and setup on the user's machine . so that mean every time the user want to access his account apiece of that software will generate a 3D shape on the user's machine itself and then transfer that 3D shape to the server side to matching it with the saved one .

4.1 How the proposed system work ?

4.1.1.user want to create an E-mail through mail provider , send request to the provider
4.1.2.provider send a piece of software to the user , the user have to instill and setup that software(this software will generate the 3D shape on the user's machine itself .
4.1.3.the provider ask the user to enter user name and fill the three fields passwords (each password should include one character and one number) . then should fill the other information .
4.1.4.the piece of software collect the passwords , first convert each field contents(character and number) to one point (one axes produced) .
4.1.5.then collect the three points (x , y , z) axes and produced a 3D shape .
4.1.6.send the 3D shape to the server of the mail provider .
4.1.7.so that is mean all the user's passwords save as a 3D shape in the server .
4.1.8.because it is very difficult to guess the actual password behind each 3D shape , so that is mean we build a strong system to avoid any an authentication violation .(see fig. 1)

4.2 How To Produce (X,Y,Z) Axes From The Three Passwords ?

first step is to create the three axes (x,y,z) from the three field's contents ,because each field consist one character and one number , actually we don't have a problem with numbers because it will considered the number is x1 axes and the character should converted into number also , we can add system to generate number instead of character because you know each character in the keyboard actually has a number by using ASCII code , so by converting each character to its ASCII code to get the number . know we have two numbers that is mean have two axes (x1 , y1) the intersection of those two axes together to produce (x) axes of the second step to be first axes to produce the 3D shape

4.2.1 Why P3D ?

Because the second step for our suggested algorithm is to generate a 3D shapes so we suggest to use Processing 2.0 mode P3D technique , we have three fields ,because each field consist two parameters (one number and one character) . convert those two points (number and character) (x1,y1) into one point (one axe) (x) axes , that's mean we will get three axes (x,y,z) from those three passwords to produce the 3D shape which is saved in the server's mail provider .

4.2.2.What Is Processing 2.0 Mode P3D ?

In Processing 2.0, there are four render modes: the default renderer, P2D, P3D, and PDF. You are drawing in 3D! In three-dimensional space, a third axis (the z-axis) refers to the depth of any given point. How far in front

or behind the window does a pixel live? Now, we all know there are no actual pixels floating in the air in front of or behind your screen! What we're talking about here is how to use the theoretical z-axis to create the illusion of three-dimensional space in your Processing window. P3D is required for this.

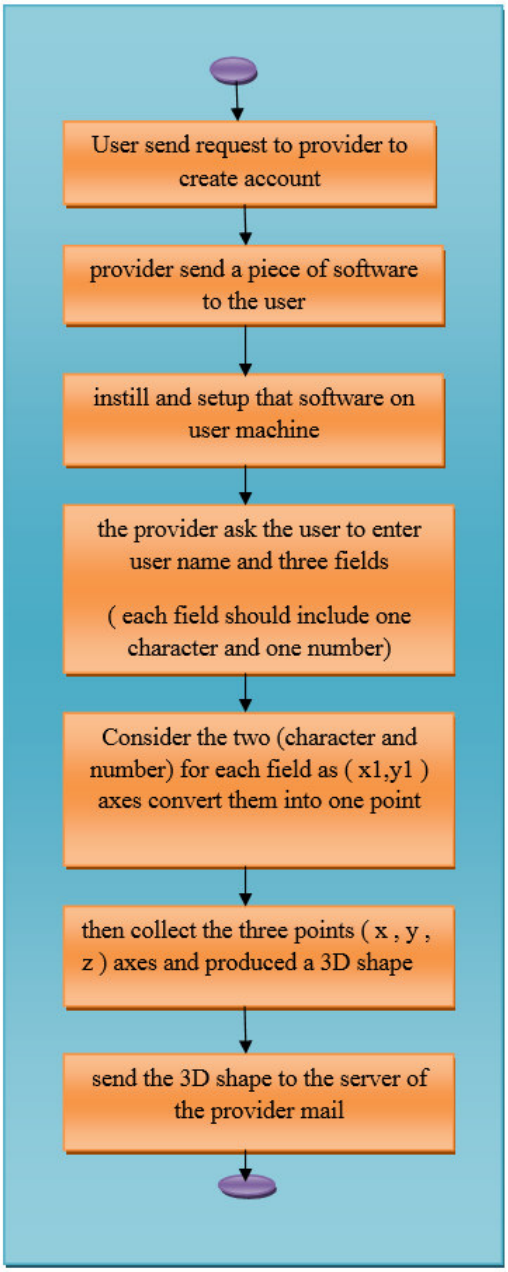

Fig 1 . Flow chart to represent the procedure

5. Analysis Of Password Secure Authentication :

5.1 Attacks & countermeasures:

As mentioned earlier our technique is most secure authentication. We will see different kinds of attacks & how our suggestion technique is more secure against different attacks.

5.1.1 Timing Attacks

This attack is based on how much time required completing successful sign-in . Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our technique is designed more securely, these kinds of attacks are not easily possible on our suggestion system because the attacker can only see a 3D shapes , can not find the real passwords & also not much effective as well.

5.1.2 Brute force Attacks

In This kind of attacks the attacker has to try n number of possibilities of a 3D shapes . As these attacks considers following two points.

- Required time to login: as in our technique time required for successful login varies & is depend on number of actions & interactions, and what are the facilities available to create a 3D shapes .
- Cost required to attack: required to know the algorithms and special software used to analyses those 3D shapes to those primary passwords , so it need costly system analyzer .

5.1.3 Well-studied attacks

In this attack attacker has to study whole password scheme. After study about scheme the attacker tries combination of different attacks on scheme. attacker fail to study whole scheme. those attacks also not much effective against our technique .

5.1.4 Key logger

In this attack attacker install as software called key logger on system where authentication scheme is used . This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password, So that this kind of attacks are much effective in this case .

5.1.5 Shoulder Surfing attacks

Attacker uses camera for capturing & recording those three password . This attack is more effective than any other attacks on a textual password. So those passwords must be performed in a secure place where this attack can't be performed. Shoulder surfing attacks is still effective & easily possible against textual password .

6. Implementation Fields

The suggestion system used to improve the security of mailing service mostly and it can applied with any accounts types need to provide security . or any type of services need to be access with machine like desk top computer , laptops , mobiles ; because of that piece of software needed to install and setup in those machines

7. Conclusion And Results

- The suggestion system provides
- Flexibility: because no need than three simple password's fields , each field consists one character and one number.
- Easy to Remember : because there are no more than six digits only so it will be easy to remember.
- Privacy : because all the password's fields processing done in the user machine before send through internet to the servers , so it will decrease the hacking to the password through sending password's fields to the servers .
- Draw Backs of proposed system
- Time and memory requirement is approximately large.
- More expensive as cost required is more than other schemes.
- More experts need to build like that system .
- Because of no need in each field to more than tow parameters (character and number) only , so the shoulder surfing attacks are effective to know the parameters .

8. References

http://www.returnpath.com/wp-content/uploads/resource/email-authentication/Return-Path-Email-Authentication-Guide-9_12.pdf
http://en.wikipedia.org/wiki/Email_authentication
Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
SECURED AUTHENTICATION: 3D PASSWORD* Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita Department of Computer Science and Engineering, Dronacharya College Of Engineering, Gurgaon ISSN 2229-600X
http://help.campaignmonitor.com/topic.aspx?t=88
https://www.processing.org/tutorials/p3d/