Pass No-Pass Graphical Authentication Service

Vikram Verma,
Computer Science and
Engineering Department
ASET, Amity University, Noida,
India

ABSTRACT
This document proposes the use of a new graphical authentication service to be used for Cloud based security, Graphical Authentication systems are not prone to key-loggers, brute-force, dictionary attacks and thus they are much secure than traditional textual authentication service, thus making a graphical authentication service would provide a good security for our data siting on cloud, against various hacking techniques. Introduction to No-Pass click points provides an intrusion detection system where we use No-Pass to lock down system and thus prevent any kind of illegitimate access to the data siting on system.

Keywords
Pass, No-Pass, Implicit Feedback, authentication systems.

1. INTRODUCTION
In today's world we are completely moving towards the Cloud for almost all the services which we earlier used to store and access from our basic computer hard drive. We wish to have access to all our data all the time irrespective of the place we are on and the device we have, thus we sync all our data to our cloud storage, but then we need to secure our data siting on cloud, thus a very good security system is needed for keeping our data away from the hands of hackers.

Authentication system is first and only major gate which authenticates user access and thus this gate needs to be the most secure. The existing authentication systems are mainly textual recall based, which have been compromised from time to time and thus we need to have a much secure authentication system to protect our data. We do have many graphical authentication systems out with proposals but they faced lots of issues, yet comparatively, graphical authentication systems are much secure than the textual ones thus it is worth to work on a good graphical authentication system and make it as a cloud service so that we can authenticate our-self remotely and have access to our data on cloud and at the same time secure our data from the hands of hackers.

The most effective graphical authentication system which is available as a commercial product is PassFaces. It has been one of the best but the issue is that the Pass Face which acts as a password are assigned by the system and thus it increases the cost of memorability for the users, thus though it is made as a commercial software it could not gain enough popularity and thus it could not get wide acceptance.

In this paper I will do a brief comparison of existing graphical authentication systems and propose my graphical authentication service from cloud perspective.

2. OUTLINE
Access control mechanisms have always been a major concern in the field of computer security, moving towards cloud has only increased its severity.

Following is a brief discussion about the existing authentication systems:

2.1 Recall Based
In these systems user needs to present the same password which he creates during the registration, user needs to present the same password at the time of login by either typing it or drawing it.

2.1.1 Textual Passwords:
These are traditional authentication system been in use since ages, they provide easiest way to enter them to the system and also provides high ease of use to the users. But they are highly susceptible to a wide variety of hacking attempts ranging from easiest shoulder surfing to sophisticated key-loggers, and brute force attacks.

2.1.2 Draw-A-Secret
In Draw A Secret[1] system user needs to draw his password on a 2D grid, he then needs to draw the exact same secret later to authenticate him, thus user tend to draw a easy to remember symmetric secrets which becomes highly susceptible to shoulder surfing attacks. And if they create a complex non symmetric then they are not able to draw it the same way during the authentication session.

2.1.3 Background assisted Draw-A-Secret
BDAS[2] was proposed by Dunphy and Yan, in this system a background image is used to assist users to draw their secrets, android pattern lock screen is one example to it, and windows 8 picture password is similar too, in these systems user either end up creating symmetric password or they choose predictive patterns on images like circling face in image.

2.1.4 Pass Shapes
Weiss and De Luca proposed PassShapes[3], in this system, alpha numeric passwords are created by drawing characters, which is later converted into alpha numeric and stored in database, it is similar to textual passwords but it eliminates the risk or leaking keystrokes, but it is still susceptible to shoulder surfing.

2.2 Recognition Based
In these systems users need not draw his password rather he would be using his recognition memory to identify his password from a set of decoy and pass images.

2.2.1 PassFaces
In initial version of PassFaces[4] users were allowed to choose their set of faces from a database of faces and then

byclicking on these faces they would get authenticated, but most users were found to be choosing predictive faces, like male chose female, race similarity in choosing faces, these were making passwords too predictive, thus in latest version of PassFaces, they assign faces to users thus predictive nature of password is overcome, but it becomes difficult for users to remember these faces as they are completely unfamiliar to them.

2.2.2 Story Based PassFaces

This system was proposed by Davis, Monrose and Reiter[5] as a comparison system for PassFaces, in this system users were asked to select a sequence of portfolio images, and they were asked to create a story by taking portfolio images to help them remember the images in the sequence, but during the study it was found that most users did not make any story rather tried to remember sequence of images and thus they were not able to succeed in pulling out right portfolio images during login in the right sequence.

2.2.3 Déjà vu

In Déjà vu [6] system users select there password images from a subset of random art pictures and users later need to select their random art pictures from shown subset to authenticate them, usage of random art increases security as it is not possible to describe their password or write them, but it also increased the cost of usability for users to remember them.

2.2.4 Geo-Pass Authentication System

In Geo-Pass[7] Authentication a map image is provided using Google maps API, and then users can choose any location as the password, studies showed that most users chose the real geographic locations as the password, for instance for password for money related accounts was chosen as their bank or ATM locations, thus it is highly susceptible to social engineering attacks.

2.2.5 Cued Click Points

In CuedClick Points[8] system users are assigned a sequence of click points on an image and they are supposed to click on these in the same sequence in order to authenticate them, this creates a high cost of memorability as click points are assigned by the system, and thus user needs to remember them, that too in the same sequence above the memorability issue there's also an issue about shoulder surfing, as user clicks on the image it is highly susceptible to shoulder surfing attack.

3. PROPOSED SYSTEM

In the proposed system, each user will have his own set of images which he will be able to upload during registration and then he would choose his pass points on these images one after the other along with he will be also mentioning his no pass points, these will be those points which if entered during the login would simply lock the account and would need user to contact the service provider for unlocking his account. There is also use of implicit [9] feedback which prevents attackers to know if they made a mistake or not during their trial of access.

During login user will be provided with his images one after the other and he would be shown some alphabets on the image at various points which would contain his pass points and no pass point along with random points on the image, now in order to authenticate user needs to type those characters in the input field which are located at his pass-points, if the user make a mistake during this by typing a character located at random point then the next image he would get for entering pass point characters will be complete out of his set of images thus he will then be able to guess that he has made a mistake and would close the login screen and start again, but if it is a hacker then hacker will not be having information about user's correct set of images so he would not be able to guess his mistake and would continue to retry and never succeed and would end up wasting his computing resources to enter into the system.

However, if user or hacker has typed the character placed on the no-pass point on the image, then the account would be locked, but as user has the information about the right no-pass points in the image he would definitely not type the no-pass character but hacker may type it and thus account would be locked and data would stay protected.

As it would be completely web based and each time new set of characters appears on the image, when used as on cloud the risk of steeling token is reduced as every time new tokens with new set of characters are generated thus any old token will not be able to provide access to the system.

4. OBJECTIVE OF PAPER

The objective and purpose of this paper is to introduce a new graphical authentication system which can act as a cloud service and provide a high security to the data and use of implicit feedback would provide a very good intrusion detection system.

5. MODULES OF PROPOSED SYSTEM

5.1 User Management:

This module deals with registering users for creating a unique ID for each user, for maintaining their images, pass, and no-pass points in database.

5.2 Password Generator:

This module provides a screen for users to choose their pass, no-pass points to createtheir graphical password.

5.3 Verification:

This module takes the unique user ID and provides user with images with characters labeled on different co-ordinates on image and a text field in which user would type the right pass point characters to authenticate them.

6. CONCLUSION

Usage of Pass and No pass click points to generate current one time password would strengthen graphical password system and implementation of implicit feedback would provide a good intrusion detection system and thus hacker would never come to know whether he is making mistakes or not, thus a highly secure and ease to use graphical password can be created in this way.

7. REFERENCES

[1] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX Security Symposium, August 1999.

[2] P. Dunphy and J. Yan. Do background images improve "Draw a Secret" graphical passwords? In 14th ACM Conference on Computer and Communications Security (CCS), October 2007.

[3] R. Weiss and A. De Luca. PassShapes-utilizing stroke based authentication to increase password memorability. In NordiCHI, pages 383-392. ACM, October 2008.

[4] PassFaces Corporation. The science behind PassFaces July 2009.

[5] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.

[6] R. Dhamija and A. Perrig. Déjà vu: A using images for authentication. In 9th USENIX Security Symposium, 2000.

[7] Using Geographical Location as an Authentication Factor to enhance mCommerce Applications on Smartphones.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle. Graphical password authentication using Cued Click Points. In European Symposium on Research in Computer Security (ESORICS), LNCS 4734, pages 359{374, September 2007.

[9] Implicit authentication, HotSec'09 Proceedings of the 4th USENIX conference on Hot topics in security Pages 9-9 USENIX Association Berkeley, CA, USA ©2009.