Graphical Based Password Using Keystroke Dynamic Authentication System For Banking Application

Kajal Birdawade, Varsha Ingale, Manisha Lole, Vrushali Mande, Prof. Mrs. DeeptiNirwal

1Department of Computer Engineering P.E.S. MCOE, Pune
2Guided By, Computer Engg. Department
PES Modern College of Engineering, Pune-05

Abstract
Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess. We are making use of encryption for sending user id and password on server from the user’s mobile phone. Once the user is authenticated he will be shown with a graphical password screen. Using graphical based technique user’s click on the images rather than typing alphanumeric passwords. User is shown with sequence of images with 4x4 blocks; user has to select N blocks from each image. We measure KDA (Keystroke Dynamic-based Authentication) for each images click. This project proposes a new graphical-based password KDA system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices. In addition, this paper explores a pressure feature, which is easy to use in touch screen handheld mobile devices, and applies it in the proposed system.

Keywords- Authentication, graphical passwords, images, usable security.

1. INTRODUCTION

The problem of Knowledge based authentication mechanism (KBAM) typically text based password are well known. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password takes images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create easy or memorable password which is easy to guess but strong system assigned password are difficult to remember. An authentication system should allow user choice while influencing user towards stronger passwords. An important usability aim of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically belief is used to control user choice in click based graphical password, motivating user to select more random click point which is difficult to guess.

In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach selects the more secure password the path of least confrontation. Instead of increasing the burden on users it’s easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is joined with previous cued click point technique which uses one click point on five different images. The next image to be showed is based on previous click-point and the user specific random value. Here the password entry is a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point. Keystroke dynamics-based authentication (KDA) systems, bring together with password knowledge and functional typing characteristics as the second identifiable factor, to achieve higher system accuracy. However, there are potential threat factors that reduce the accuracy and portability of the KDA system. That is, some portable computational devices do not have standard desktop keyboards such as personal digital assistants and mobile phones, resulting in a reduction in system portability if the enrolment phase is implemented based on the desktop keyboard. Differences in computers, for example, desktop versus laptop, may lead to significantly different typing performance and therefore affect the accuracy of KDA systems. Recently, artificial rhythms have been used to improve the keystroke data quality, for instance, a pause between characters. The user in this system should memorize the locations of pauses inserted in his password. Because this is not an innate typing characteristic, a personalized rhythm click dynamics-based authentication system is proposed in this system.
2. Related work

<table>
<thead>
<tr>
<th>Sr.No</th>
<th>Author Name</th>
<th>Used Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Uma D. Yadav</td>
<td>CCP[Keystroke Dynamics]</td>
</tr>
<tr>
<td>2</td>
<td>Ting Yu</td>
<td>Continuous And Static Verification[Mouse Dynamics]</td>
</tr>
<tr>
<td>3</td>
<td>Max Well Krohn</td>
<td>Proactive Digital Signature[Signature]</td>
</tr>
<tr>
<td>4</td>
<td>Smita Das</td>
<td>FFT And DFT [Voice]</td>
</tr>
</tbody>
</table>

Dwijen Rudrapal, Smita Das, S. Debbarma, N. Kar and N. Debbarma investigate in their “Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People”. Voice biometric is unique biometric of every human being. It is numerical model of sound, pattern and rhythm of voice. While entering in system it stores two recording of user. When user log in system it compare with both the stored recordings. Comparing is very tricky task for the system. For that they use DFT and FFT transforms. And also uses Butterfly algorithm for Fourier integral transforms [7].

Zach Jorgensen and Ting Yu investigate in their “On Mouse Dynamics as a Behavioural Biometric for Authentication”. In mouse dynamic two methods are used but there are disadvantages on the system of mouse dynamics. Continuous verification requires amount of mouse data to be captured before authentication. Limitation for environmental variables. That when using another machine there are different software related and hardware related variables. There occurs problem in remote access scenario due to variety of mice that impact the performance of authentication. Mouse movement can be easily seen by attacker so authentication using mouse dynamic is less secure [5]. Antonio Nicolosi, Maxwell Krohn, Yevgeniy Dodis and David Mazi` res investigate in their “Proactive Two-Party Signatures for User Authentication”. They perform 2 parts client and server to produced signatures. And can be refresh the shearing of private key. Exchanging of private key from client to server is very not easy task. Speed and stress impacts on of signature. In signature authentication, there is high error rate [6]. Uma D. Yadav and Prakash S. Mohod investigate in their “Adding Persuasive features in Graphical Password to increase the capacity of KBAM (Knowledge Based Authentication Mechanism)” In that images can be used in authentication. In this user when log in system it provides images to the user one by one. Image is divided into matrix. User has to select the correct point and if he selects incorrect point then the next image will be incorrect. Authentication using image is very useful and graphical password is easy to remember. In this technique, we used clued click point means selection of image point that’s why it is more secure [1].

3. Motivation

Now a days security is more important. Textual password can easily hacked by attackers. Graphical password can easily recognized and memorized by human being. So we built a system that will take textual password as well as graphical password. There is only CCP in one of existing system. We have added keystroke dynamics in CCP. Every person has different typing rhythm. So keystroke cannot be hacked by anyone.

4. Methodology

In this paper following 3 algorithm are used

A. AES Algorithm.
B. Graphical Authentication Using CCP.
C. Keystroke Dynamics Authentication (KDA).

A. AES ENCRYPTION ALGORITHM

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Like its predecessor DES, AES does not use a Feistel network. AES has a confirmed block size of 128 bits and a key size of 128, 192, or 256 bits. By difference, the Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4 x 4 column major order matrix of bytes, termed the state while some versions of Rijndael have a larger block size and have additional columns in the state most AES calculations are done in a special finite field. The key size used for an AES cipher identified the number of repetitions of transformation rounds that convert the input into the final output is called as cipher text. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128 bit keys
- 12 cycles of repetition for 192 bit keys
- 14 cycles of repetition for 256 bit keys

Each round consists of several processing steps each containing four similar but different stages including one that supported bytes on the encryption key itself. A set of move backwards rounds are applied to transform cipher text back into the original plaintext using the same encryption key [1].

B. GRAPHICAL AUTHENTICATION USING CCP:

a) User Registration

i. User allows selecting N unique images.
ii. Select cued click point on each image.
iii. Store cued click point in database.

b) User Login

i. Display images in sequence.
ii. Select cued click point on each image.
iii. Check register CCP and new CCP are same or not, if CCP points are same then display next right image else display image from other images [1].
C. Keystroke Dynamics Authentication (KDA).

a) Down-Up (DU) time:
DU time is the interval in the same click being pressed and being released [Fig. a].

b) Down-Down (DD) time:
DD time is the interval in the click being pressed and the next click being pressed [Fig a].

c) Up-Down (UD) time:
UD time is the interval in the click being released and the next click being pressed [Fig a].

d) Up-Up (UU) time:
UU time is the interval in the click being released and the next click being released [Fig a].

e) Down-Up2 (DU2) time:
DU2 time is the interval in the click being pressed and the next click being released [Fig a].

6. Conclusion
A major advantage of investigate scheme is that it provides larger password space than the textual passwords. For Graphical passwords there is an interest that they are more secure than the textual passwords, while the important argument for graphical passwords are that people are better to memorizing graphical passwords than textual passwords. Also it eliminates the pattern formation and hotspot attack since it provides the system suggestion. Also the investigate system eliminates the shoulder surfing attack.

Future work

References


[6]. Antonia niolosi, Max Well Krohn, Yevgeniydodis, "Proactive Two Party Signatures for user authentication”