MULTI-FACTOR AUTHENTICATION USING GRAPHICAL PASSWORDS THROUGH HANDHELD DEVICE

P. Shyam Sunder¹, Ballikonda Sai Chaitanya², D. Vijay Kumar³, P. Satya Shekar Varma⁴

¹,²,⁴Department of Computer Science and Engineering, MGIT, Hyderabad, India
³Department of Information Technology, MGIT, Hyderabad, India

ABSTRACT:
Single factor authentication is no longer secure in this digital environment. To gain access over a system is very easy for single factor authentication. So to ameliorate the level of security we have to expand the access to the information. In this paper we propose a system of multifactor authentication by using both traditional Alphanumeric Password and Graphical Password as gateway for authentication. We like to introduce an adaptable software Ozeki NG SMS Gateway which enables applications to send SMS messages directly to a mobile phone. This approach can also decrease the user’s effort to memorize the password.

Keywords: Authentication, Multi-Factor Authentication, OZEKI NG SMS Gateway, Graphical Password and OTP.

[1] INTRODUCTION

The term authentication can be defined as validating someone’s identity. The authentication methods till date are based on something that can uniquely represents the user (biometric characteristics), something that user already knows such as PIN. Basically, a user accessing a system should know his/her user name and password to access the system. If the username and password pair is matched correctly he/her will be granted to access the system. But this approach is done by keenly observing several facts of drawbacks like the user generates an easily guessable or a very weak password. The defect also ranges from like user having same password for multiple accounts or storing them in a system or asking web browsers to save passwords for their accounts. Today most of the software industries rely on static password to verify user’s identity. Due to the defects and static password it gives a chance for hackers to crack users password using various techniques such as guessing attack, shoulder surfing attack, dictionary attack, brute force attack, snooping attack, social engineering attack etc. To solve the problem of static password in banking sectors and for online transaction two factor authentications using OTP and ATM pin / cards have been implemented.

In two-factor authentication the user has to provide something that user has that is card along with typically memorized password, whereas in multi-factor authentication a user has to pass through multiple barriers for verifying his/her identity. Thus multi-factor security framework provides a better facility for authenticating user’s identity. The main target of
Multi-factor authentication is that to provide a more defensive layer and make it more problematic for an unauthorized person to access a system or target location. If one of the barriers is put down, the attacker has to still pass to another barrier for reaching the target location. Multi-factor Authentication is a system where in two or more diverse factors are used in combination to authenticate.

At present to overcome the limitations of static password or two-factor authentication, many organizations are turning themselves for adopting Multi-factor authentication. In the present paper, we mainly focus on Multi-factor authentication using graphical entities along with the combination of OTP generation for increasing the security for authentication.

When compared to the traditional 8-character textual passwords, this system provides a higher space of required password combinations. Because this can reduce attacks, mainly brute-force attacks, dictionary attacks, and keyboard sniffers. The scientists suggest that pictures are very easy to remember than textual things. Thus graphical passwords reduce the load of memory stress on users and provide higher combinations of password.

Multi-factor authentication is done by combination of the static password method with some other factors such as One Time Password, Handheld devices etc.

In this paper, we propose a technique by combining both multi-factor authentication and graphical passwords. This technique overcomes the restrictions of traditional 8-character textual passwords method. Here we combine graphical password with a handheld device, so that can enable to provide a secure authentication.

[2] MULTIFACTOR AUTHENTICATION

Let us first discuss about the differences between three concepts, they are, Single Factor Authentication, Two Factor Authentication, and Multi Factor Authentication (MFA).

A. Single Factor Authentication:-

Single Factor Authentication is a method which uses only a single factor i.e. a password to validate a user who is logging onto a system. This is “something a user knows”. The biggest advantage of this is its simplicity, speed, and ease of use.

B. Two Factor Authentication:-

The Two Factor Authentication in addition to the first factor i.e. username and password combination, the second factor is “something a user have” – such as a mobile phone. The advantages are it provides a great security, hackers are not so good in this technique.

C. Multi Factor Authentication:-

The Multi Factor Authentication (MFA) is basically a combination of two or three independent credentials to validate a user. This is “something a user is” – such as a fingerprint, a retina scan. The main advantage is to protect the user against identity theft and fraud done in major cases.

In the following section, we explain the terminology being used further in the paper.
In present digital environment the static passwords are not enough for authenticating a user because these are easily guessable, hacker can easily crack the static password. To ensure proper security we are proposing to implement OTP for increasing the security layer.

Procedure is as follow:

Step 1:- User enters his username and password in the login page.

Step 2:- After completing the first step, the user’s mobile number is looked up in the database.

Step 3:- if the user’s mobile number is found then OTP is generated using some function and sent to the user’s handheld device.

Step 4:- Then the user enters the OTP sent by a function to finish the first phase of authentication in system proposed by us.

One Time Password can contain random numbers, alphabets or combination of both. As these are generated by the server these are not easily guessable. The main advantage of OTP is that they are not constant they change constantly for specific period of time.

For implementation of a tremendous SMS gateway software to send the SMS messages containing the OTP to user’s mobile devices we are introducing OZEKI NG SMS Gateway.

Implementing OZEKI NG SMS Gateway:

OZEKI NG SMS Gateway is a software that can be simply installed on any computer and using this we can directly send SMS messages to a mobile phone.

Preconditions:-

To implement this solution, there should be a connection between the mobile network and the system. This connection can be established in two ways:

By using an Internet connection or

By using a wireless connection by attaching a GSM modem to your PC or GSM phone.

1. Requirements for Internet based connection to the Mobile network:-

The following devices are needed to create the connection between a system and an SMS service provider via the Internet:
So, initially we need to select an SMS service provider who guarantees Internet based SMS services. After deciding a specific provider and service, we need to sign a contract and then will receive some connection limitations from the provider. If these are properly taken then we can layout our Ozeki NG SMS Gateway software.

2. Requirements for wireless connection to the Mobile network (GSM modem):

With this type of connection all we need is a GSM mobile phone or a GSM modem, so that we can simply with a data cable we can connect it to a PC. The Ozeki NG SMS Gateway software operates the GSM device and takes care of the whole SMS messaging wirelessly. The required components to build this type of connection are given below:

Internet based connection vs. wireless connection:

In wireless connection (GSM mobile or GSM modem), SMS messages are sent through radio waves, wherein internet based connection SMS messages are sent through the Internet to the Short Message Service Centre (SMSC) of the mobile network operator.

Sending SMS messages using a wireless connection (GSM mobile or GSM modem) is a well secured technique. Because it is hard to catch and decode the message. If they are sent using internet based connection, to an SMS service provider, VPN is setup between our Ozeki NG SMS Gateway installation and the Short Message Service Centre (SMSC) of the mobile network operator.

To build a secured system it is better to implement both of these systems by configuring a backup route in our Ozeki NG SMS Gateway software.

Advantage of using above specified method is that we can securely transfer the OTP to the user and avoid hacking. Even if the phone is stolen containing the password, since the password is valid only for a specified session and cannot be used further there is no problem to consider.

[4] TERMINOLOGY

In our approach we are considering three terms: handheld, node and server. Handheld is nothing but an entity or an object that is easily carried by the user. Basically it can be a mobile phone or tablet or any other device having a graphical screen capable of displaying...
images. Instead of using the terminology mobile phone or any other term we will consider the rest of the paper the term “Handheld”.

The online service provider is nothing but a server. It offers authentication mechanisms to the user. If the offered authentication mechanism is successfully completed by the user, then he/she is said to be authorized and gets accessed to resources.

Node is used to extend the services provided by server. It is a computing device which have a graphical screen and pointing input device e.g. touch screen. We have two options for the node:- public node or private node. By using the public node the threats for our system are somewhat more when compared to the private node.

Here the authentication in graphical password occurs through two images:- key image and password image. A copy of password image is a key image. The key image is sent to the users handheld and the password image is shown on the node. The key image contains the key points where the user has to click on the node graphical screen using pointing device for authentication. Here the number of key point or clickable points specified are encrypted by the server.

[5] IMPLEMENTATION AND SYSTEM DESIGN

The implementation part and system design of proposed model is as bellow:-

Here in our proposed system the authentication process starts by entering the username and password. Then it is redirected to the Authentication Server, so that it creates an OTP message based on the user’s identity by using a cryptographic hash function. Then through SMS the OTP generated is sent to the user. Here we are using OZEKI NG SMS Gateway to send the OTP to the user.

In the first gateway User then enters the OTP in to the browser. The OTP is verified by the authentication server, if it is matched then he/she is directed to second gateway.

In the second gateway, the user gets a graphical image (key image) on handheld. For completing the authentication process, the user clicks on the specified spots on the node of the image generated on handheld. Then user is given access to account where user can upload and download data and later logout.

Figure: 4. Interaction between node, server, handheld, user.
[6] ANALYSIS OF SECURITY AND KEY SPACE

By using the above scheme it is impossible to guess the password and hack the password e.g. password eavesdropping.

Mainly it becomes very hard to the brute-force attacks, dictionary attacks and keyboard sniffers. The authentication structure is too complex, because the number of minimum click points required and number of unique clickable areas in the password image are unknown.
Basically, the size of key-space depends on number of clicks and number of clickable areas. If these are increased then size of key-space also increases. Consider there are ‘c’ click points and ‘β’ clickable areas then we have \( \beta^c \) combinations of password which is highly impossible to guess.

For example if the password length is 6 clicks and there are 25 clickable areas then the number of potential combinations can be calculated as: \( P = 25^6 = 24,41,40,625 \). As the number of clickable areas increases potential combinations also increases.

To make it easy for the user to identify the password in the image we can incorporate the user defined password into the image e.g.

![Example of user password encoded into image](image)

**Figure: 6. Example of user password encoded into image**

Shoulder surfing
In this proposed system even knowing one’s password we cannot access to their account because password changes every time and because of usage of handheld screen size is very small it is highly not possible to look into their diminished screen and remember the password. Hence this method provides a solution to the problem of shoulder-surfing.

Keystroke logging
This is a method of recording the key struck on a keyword. This method is also called keyboard capturing or keylogging. In our proposed system we use OTP method and point the device to click password and hence this cannot be affected by keylogging.

Dictionary attack and Brute-Force attack
According to the study for graphical password it has a way to hacker to hack based on generic user hot-spots. So, hence in our proposed system the password is generated by system and there can be no topic of hotspots here. Hence the problem of Dictionary attack and Brute-Force attack is also solved.

Social engineering
Social engineering is quite a non-technical method used by hackers that mostly relies on human interaction, like tricking the people to know their personal information e.g. password.

Our proposed system eliminates the problem of social engineering because there is no participation of user in generation of password, the system itself generates the password. Because of no user involvement in the generation of password, proposed system eliminates the problem of social engineering.
What if handheld is stolen or lost?

In our proposed system as explained in the figure 6, the system can encrypt user defined password into the image. So the user can only easily identify password. Even if handheld is stolen or lost there is no problem as the encoded user defined password can only be known by the user which can be e.g. Secret letters or PIN.

Comparison of our proposed system with other graphical password systems.

<table>
<thead>
<tr>
<th>Issues</th>
<th>Other systems</th>
<th>Proposed system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shoulder-surfing</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Keystroke logging</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Brute-force attack</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Dictionary attack</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Social engineering</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

[7] CONCLUSION

This paper presents a new authentication scheme based on graphical password and multifactor authentication. This approach is mainly implemented to increase reliability, security of accessible authentication mechanism for public users. The advantages of this new authentication scheme are as follows:-

- It eliminates brute-force attack.
- Handheld device is trusted as it was never before.
- This authentication scheme resists shoulder surfing.
- This authentication scheme resists screen recording attacks also.

Through our proposed system, the system cannot learn about password as it is generated by authentication server and so we can easily store confidential data through the system.

REFERENCES


[10] Ziqing Mao, Dinei Florencio, and Cormac Herley “Painless Migration from Passwords to Two Factor Authentication” in 'WIFS’ , IEEE, Brazil, pp. 1-6, Nov 29th-Dec 2nd, 2011


