Comparison between Graphical, SPAKA+, Strong and Hybrid Password-Based Authentication

[1]Vaijayanti Kulkarni, [2]Anamika Singh, [3]Rahul Kumar Chawda
[1]MCA Student, [2]MCA Student, [3]Head of Department
[1]Computer Science Department,
[1]Kalinga University, New Raipur, Chhattisgarh, India

Abstract: As the generation of the system evolved, so did the fear of system break-ins. Due to the low security in password protection, we only enabled attackers to enter in our system. In order to improve the password authentication and for the betterment of the same, many methods are introduced. But how can you claim that the particular method is much better than the rest? In this proposed paper, we have described a comparison between few methods and find the one which is comparatively stronger in password protection than the rest. This paper does not propose any new method but Compare the ones that are already available. In this paper the comparison is mainly done between graphical method, SPAKA + method, strong method and hybrid method of password based authentication. We have explained the working of the given methods and compared them to come to a conclusion.

IndexTerms **- Graphical, SPAKA+, Hybrid, Strong, Password-based authentication, Point-of-Interest (POI).**

I. INTRODUCTION

We live in the world where Technology has advanced to its highest level. And to secure our data from phishers we mostly use passwords. Using password, it only provide access to the authenticated users. This is mainly known as Password-based authentication. The primary motive is to provide more strength, not replace the password-based authentication. Many methods have been introduced for the same. But there is a lot of confusion for what to use as the best method for the password based authentication among them. In this paper, we describe four methods and compare each one to know which method is suited as the best. Mainly comparison is done between graphical method, SPAKA+ method, hybrid method and strong method.

When the phishers succeed in guessing the correct password, it's called 'online dictionary attacks'. When the phishers has to summon messages between the users and server or find a copy of password file it's called 'offline dictionary attacks'.

II. Explain used methodologies?

2.1 Strong password: - In strong password, the user does not need to type his password instead he has to enter a password identifier to login. Because of this method the attackers have no idea about the exact password of the user which keeps the information safe. It reduces online dictionary attacks and eavesdropping attacks.

2.2 SPAKA+ method:-User always choose easy password that he / she can remember for long term, which can be guessed by attackers easily. So, to protect user's information we use SPAKA+ method. SPAKA+ stands for strong password based authentication and key agreement. SPAKA+ method increases the computational burden for the attacker. That means in case the password entered is wrong, the attacker has to solve equations and puzzles.

2.3 Graphical password: - Another method is graphical password. Graphical password provides a way to use pictures as passwords, because pictures are easily remembered then words. In such systems, user create password by clicking on several preferred location of an image. If the user has to login then he has to click on those locations which he selected, previously. Alphanumeric passwords are easily guessed by attackers, so graphical password provides a better security to the user.

2.4 Hybrid method: - The last method is hybrid method. Hybrid method is normally the combination of two or more method. For example, all the above three Method can be used altogether to create one hybrid method. Hybrid method is considered as comparatively better than the rest of the method.

III. Implementation

To understand the working of these methods, we have created a login page using Visual Basic 2010. The form simply consists of two main components:-

(I) User ID, and

(II) Password.

In every method, User ID remains unchanged, whereas Password field is changed accordingly.

3.1 Strong Password:-

In strong password method, the user enters the password without actually revealing the password. We have demonstrated this method in the following way:-

A login page created with the help of strong password method. Here the user has to enter his User ID and password identifier to login. In this way, the attackers have no idea about the actual password.

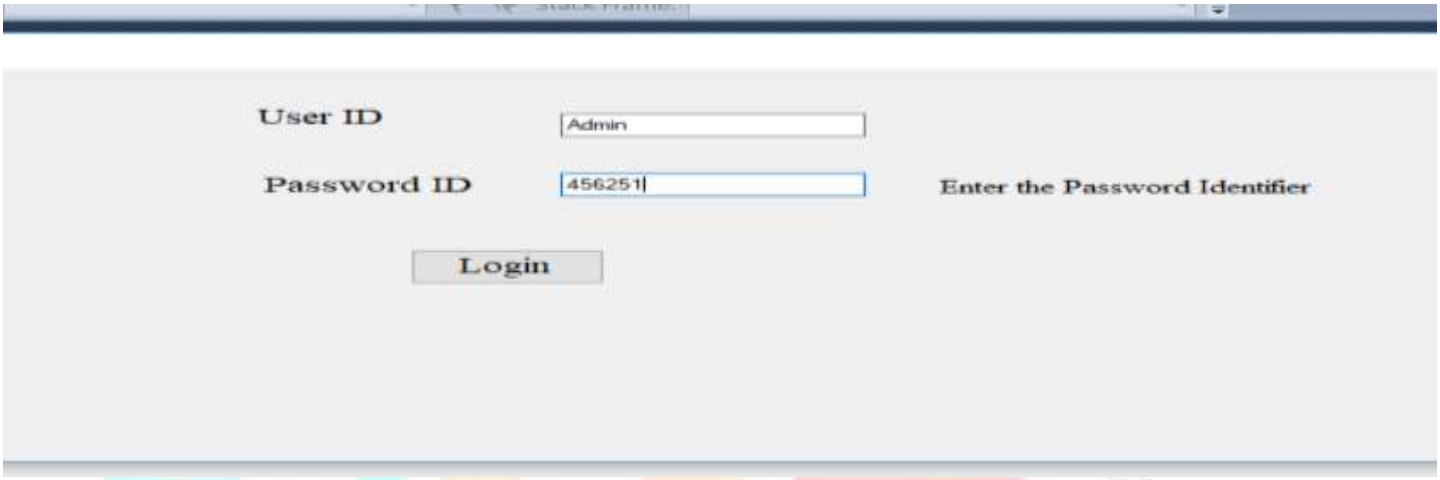

Figure 1.1 strong password method of password-based authentication

3.2 SPAKA+ method:-

SPAKA + Method are known to increase the computational burden of the attackers. We can demonstrate this method in the following way:-

A login page is created using SPAKA + method. Here, if the attackers enters wrong password then a window will pop up, containing puzzles in it. So, the attackers have to solve the puzzle to get through.

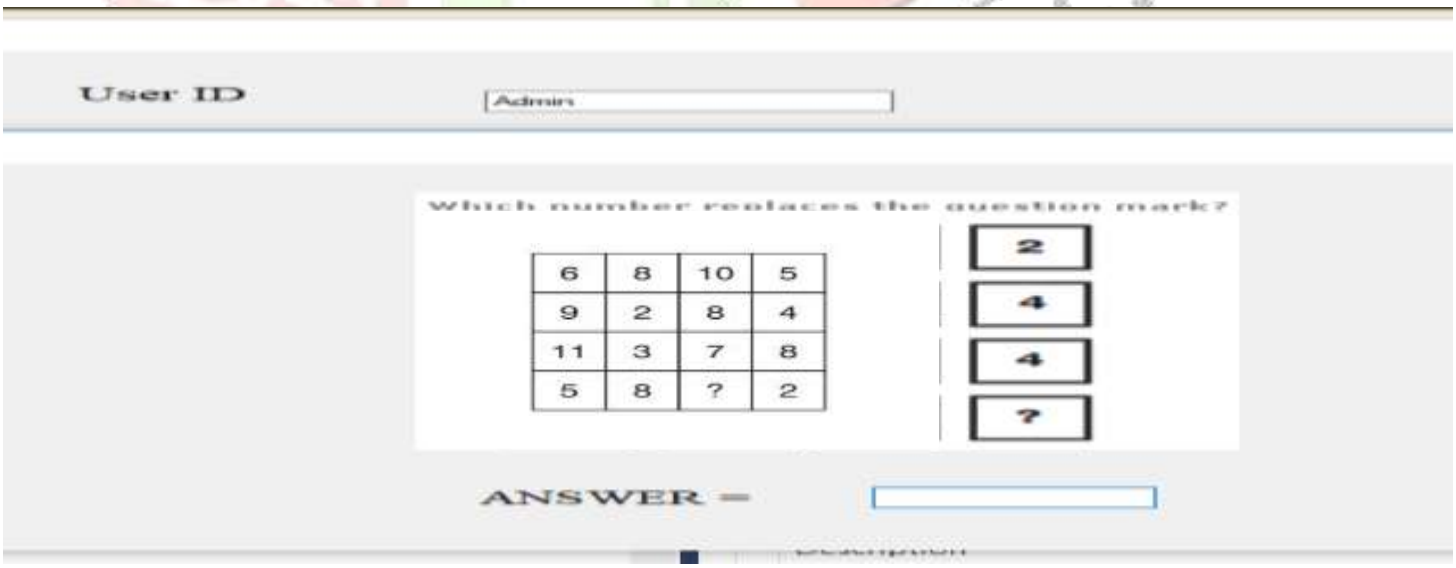

Figure 1.2 SPAKA+ method of password-based authentication

The following puzzle gives the result =12. As you can see across and down, in each line of four numbers the sum of the first two numbers is one less than the sum of the second two numbers. So the attacker will have to solve this puzzle to get through.

3.3 Graphical password:-

As the name suggests, Graphical password uses graphics, images and drawings as password. The given Method can be further explained as follows:-

A login page created using graphical password. Here, instead of password block there is an image in which user is supposed to click in several predefined location then only user can access information.

Figure 1.3 graphical password method of password-based authentication

3.4 Hybrid method:-

Hybrid method is normally a combination of two or more methods in following way, we can understand hybrid method:-

A login page is created with the combination of strong password method, SPAKA+ method and graphical method. Here the computational as well as mental burden is increased of an attacker. First the attacker has to enter a password identifier; if it is wrong then a window will pop up with a puzzle. The attacker has to solve the given puzzle, if not then image will pop up. Then attacker has to click on several locations which are already decided by the user and if the attacker fails in doing so the session will be expired and attacker will be blocked out of login page.

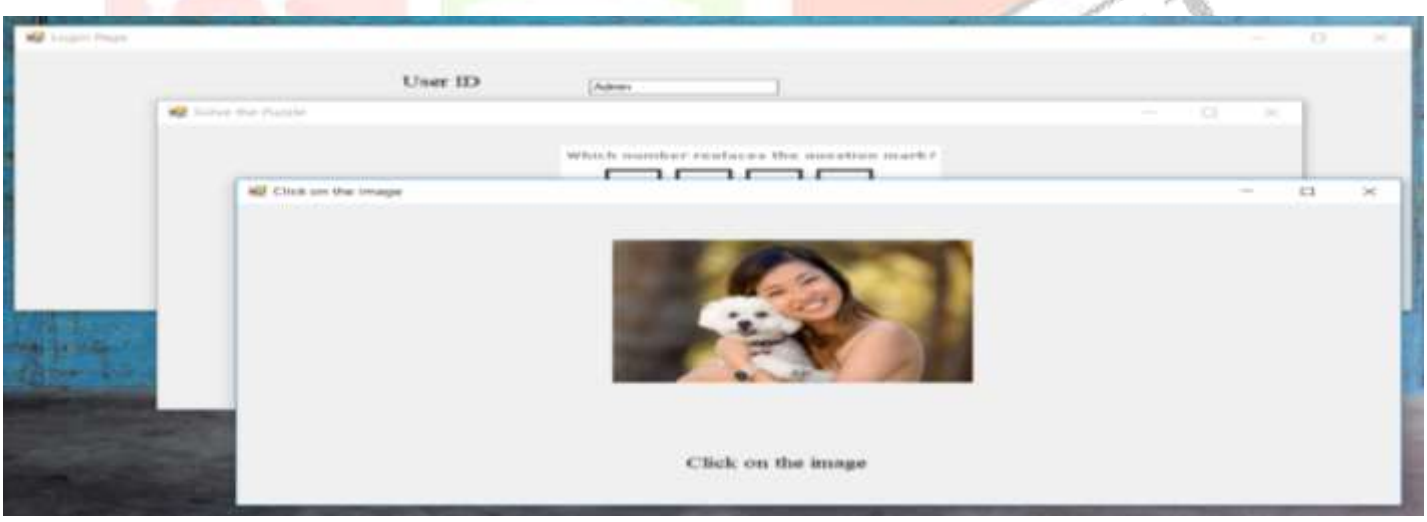

Figure 1.4 hybrid method of password-based authentication

IV. Comparison of methods

4.1 Comparing strong password and SPAKA+ method:-

In strong password method, the user has to enter a password identifier instead of entering an actual password, but this method is not entirely safe as attacker can guess or find out password identifier using different methods. So, the SPAKA+ method was introduced to increase the computational burden of the attackers where the attacker has to solve the given puzzle. The attacker can easily guess the password identifier but he will have to put more effort and time in solving the puzzle. So, comparing both the methods, SPAKA+ method is better than strong password method.

4.2 Comparing SPAKA+ method and graphical password method:-

In SPAKA+ method, the attacker has to solve the puzzle or any algorithm set by the user. But this method too is not safe as the attacker can be an intellectual and it would be easy for him to solve any puzzle, whereas, in graphical method the user create password by clicking on several point-of-interest (POI), which can be very difficult for attackers to guess. So the graphical password method is considered as the better option.

4.3 Comparing graphical password method and hybrid method:-

In graphical password method, the attacker will have to guess the point of interest (POI); if he is lucky enough to guess the right points then he will be able to access the files and information of a particular user. Because of which graphical password Method can also be not considered as safe option for password based authentication. It has been discovered that all the three methods i.e. strong password method, SPAKA+ method and graphical password method are not entirely safe. But if all this three methods are combined to form one hybrid method then they can increase computational as well as mental burden of an attacker. And if he fails to compute all the puzzles, POI and password identifiers, then he will be instantly blocked. So, we consider hybrid method as the safest method for password based authentication. Hybrid Method can be understood easily by the following flowchart:-

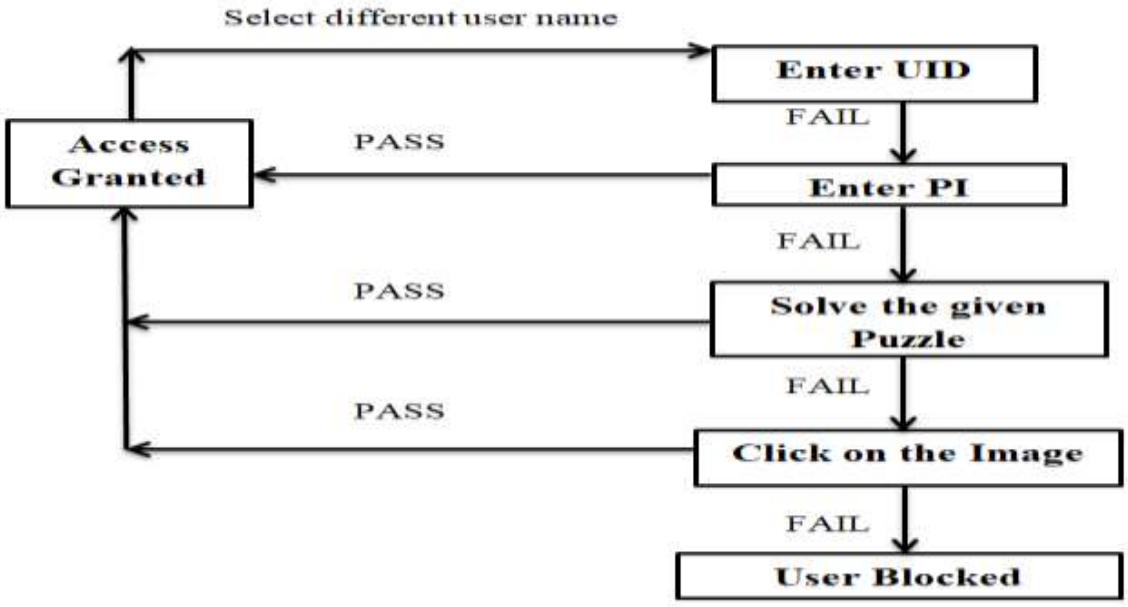

Figure 1.5 flow chart of hybrid method of password-based authentication

V. Conclusion

In this proposed paper, we have compared the strong password methods, SPAKA + method, graphical password method and hybrid password method, and came to a conclusion that hybrid method is far better and safe than rest of the methods. For the computer security as well as user's security, password based authentication is the fundamental component. We need a method which can be more safe, secure, robust and reliable. So combining two or more methods, password based authentication will become so secure that it will keep away the attackers.

VI. References

1. Strengthening Password-Based Authentication Protocols against Online Dictionary Attacks by Peng Wang, Yongdae Kim, Vishal Kher and Taekyoung Kwon.
2. Strengthening Password-Based Authentication by Scott Routi, Jeff Anderson and Kent Seamons.
3. A Graphical Password-based Authentication based system for mobile devices by Er. Aman Kumar and Er. Naveen Bilandi.
4. Secure User Authentication & Graphical Password using Cued Click-Points by Miss Saraswati B. Sahu and Associate Prof. Angad Singh.
5. A Graphical Password Authentication System by Ahmed Almulhem.
6. Cryptography & Network Security by Behrouz A Forouzam and Debdeep Mukhopadhyay.
7. Network Security Essentials by William Stalling.