"SELF AUTHENTICATION" AN APPROACH FOR PASSWORD FREE AUTHENTICATION

Prabhakar Gantela
Department of Information Technology,
Mizan Tepi University,

Tefera Adugnaw Lulie
Department of Information Technology
Mizan Tepi University

Abstract* — Authentication has always been a topic that is challenging the researchers and the computer experts as daily we have news of hacking the sites or the internet accounts. Fifty years passed since we have passwords on the computers but still security is unsecured. We have many techniques in authenticating a user to his account but still there has been always a way out for the hackers to log into our account. Even though we have various methods to cross check the user, the accounts are still not safe. We have lot of cryptographic techniques, digital signatures, OTP (one-time-passwords) but none is helping us in this regard. There are many reasons that make our account hacked but what we propose is that the password load that we impose on a user may be one reason that makes our account unsecured. As any user now a day has many accounts, they try to use an easy to remember password and that's the loophole that gives hackers a chance for hacking. In this paper, I propose a new method where there will not be any password for logging in. The user will be burden free of passwords. This is a trial to make the authentication simple and secured. We proposed a method called self-authentication in this paper where the user himself becomes a password for his account. A set of questionnaire is posed on to user will be taken as a sample and the answers given by him will decide his password for his next login. We think this method helps us in avoiding passwords for authentication.

Keywords— Authentication, Passwords, Security, Cryptography, brute force attacks, password policy, bystanders, guessed passwords, man in middle attacks.

I. INTRODUCTION

Since the day authentication has been started, the method used to identify a user has been changing. The word that comes into mind when we hear authentication is security. As the history says from 1960's when we started having individual accounts on a system we started working on these user names and passwords. But the key point is how can we identify a person in this huge world of Internet. Identifying a user has been always a question mark. The user has to show that he is the only one separate from this world.

A password is defined as a word or a string of characters used for the user's authentication to prove identity or access approval to gain access to a resource which is to be kept secret from those not allowed access. The word secret is the main problem. To maintain this secrecy, we have been working for years. We have many techniques to maintain these secrets.

We have text passwords, voice recognition, Bio metric, Iris and also face recognition techniques. Now a day we have image authentication, video authentication and device authentication techniques. Even though we are stuffed with these many methods of authentication, still our accounts are not safe. Still we hear hacking news once in a day. There may be many reasons how our account has been hacked. But one reason I strongly believe is the overload of passwords that we impose on users may be one key point that helps the hackers in entering into our accounts.

Now a day's any computer user or any online user may have at least twenty plus accounts which may be their email, social networking sites like face book, twitter etc, laptop passwords, mobile passwords, bank ATM Pins, email etc. Each user has more than one account in each site. These make the user overloaded. On a whole, the user is forced to remember his passwords every time they log in. To remember these passwords, they are using easy to remember, poor strength text passwords leaving a hole for the hackers to enter. As they have many accounts and many passwords, the users tempt not to follow a strong password or a password policy.

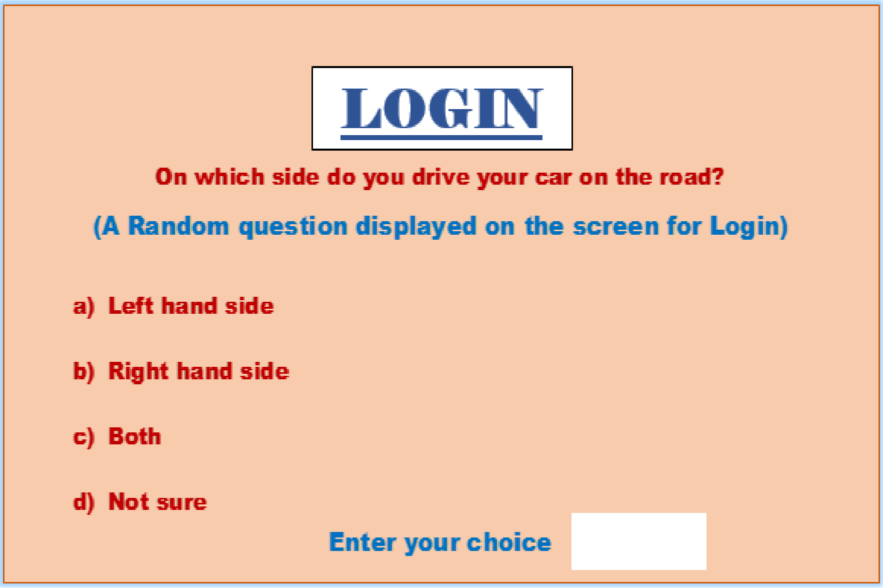
We proposed a method called *self-authentication* in this paper, which we think, helps us in avoiding passwords for authentication. The main goal of this process is to create a password free world and make users burden free and reduce their overload of remembering the passwords. As an initiation, we have followed a mechanism of reading the user psychology for proving himself for authentication.

II. IMPLEMENTATION

Authentication has to be done but without passwords. The main problem here is to identify a user with some information which is known only to him. This can be his personal data, secret pin or some code that can be used for identification. Our study in this regard has been for years and finally came up with this self-authentication which we think might help us. We have used our body parts as passwords such as our voice (voice recognition), eyes (Iris), face (face recognition), and hands (Bio metric authentication). All these parts are used as passwords for our identification. All we tried is to prove ourselves to enter into our account. But what we missed here is “it is only you who can prove who you are”. None in this world can be you except you. None other can think and react exactly like you. It is you who can be you in this world. “Why can’t be you as your password for your Account-*Self Authentication*”.

The process begins from the step the user registers into a site or an account. While entering his data during registration he may be asked to enter his first name, last name, mobile number, date of birth etc. In many of the sites he will be asked to select a password and retype it for confirmation. Instead of doing this in self-authentication, we will ask few questions from various angels that may be how he behaves and reacts to a situation or how he behaves with his relatives, friends and others who are not related to him. On a whole we try to capture the way he thinks and behaves. We study his mind with these questions. These questions may be nearly ten with which we can get a clear picture of what he is and how he is and how he behaves and reacts. It is like a psychology game where he will be captured completely by the questions we pose to him. Even though the process may take time but remember that it is only for the first time he spends his time while registration.

Later when the user tries to log in with his user name, he will be posed a random question on the screen. This question will be purely random and even the user doesn’t know what the question and answers are. The question may be any situation or may be a suggestion to a problem from the user with which we try to match his thinking from the data he entered while registration. The data which he entered and answered while registration will be correlated with the question and answer he has given while logging in. The answer will be matching with his way of thinking and only on matching he will be logged in. If the answer he entered is mismatched, then the system identifies that it is not the exact user who registered.



LOGIN

On which side do you drive your car on the road?

(A Random question displayed on the screen for Login)

a) Left hand side

b) Right hand side

c) Both

d) Not sure

Enter your choice

Fig 1. Random question displayed on Login screen

Let us take an example of a user who registered himself with a false attitude and who acts smartly and tries to convince others as if he is a gentleman. But at the time of registration, his mindset will be captured and his original nature is recorded by the authentication mechanism.

Now for the example figure given above the user tries to act smart and selects a choice proving himself to be loyal to the traffic rules.

But as per the authentication mechanisms records he will be rejected on acting wise saying he drives on to the right hand side (International driving standard) and proves to be strictly following the rules. But as he is wrong to his nature he will be rejected from logging in. He will be logged in only if he behaves according his true nature and mindset and only on entering the correct option according to his nature and attitude.

If a hacker tries to enter into others account, even if he knows the user name or has bank ATM with him, the question which displays on the screen will be new to him. For the question he may answer in his way as he may not know how the original user thinks, reacts and how the user behaves. It is only the registered user who can answer exactly to the question displayed on the screen. Even if the hacker tries to manage and think like the registered user, he may be close to the way the user thinks but not exactly.

The Login process has the following metric. While registration depending on the question and answers the user will be placed in a set of categorized persons. When he tries to login for the next time the user will be posed a question for which one category of question and answer is expected. The answer he gives for the question should be between 90-100% of his mentality and psychology. We took a margin of 10% as grace because even the registered user may not be having the same sort of mood which he had while registration. So when he tries to login he should be 90% exactly as he is while registration.

If a hacker tries to login with the user name of others, he will be asked to answer a question for which he has to match the thinking and behaviour of 90% and above. Even if he manages to behave and think like him, he may be almost up to 50-70% like the registered user but not 90% or more. This makes the user safe with his account. The system checks the answer and finds the percentage of correctness in the answer with the registration. If the answer matches he will be logged in, and if not rejected.
This approach has two advantages – one is the user need not remember his password or need not follow any password policy and the other is his account will be secured and safe.

III. RESULTS OBTAINED

To work on this, we have taken a sample of few of my students for registration. we have prepared few questionnaires and asked them to answer. Few days later, we gave them a question randomly and told them to answer it. We correlated the answer with the key, which we already had with us. Surprisingly this case study works and almost 65% of the student's answers were matching with the answer, which we expected. The remaining answers, which were not matched, were almost close enough to what we expected. This was encouraging us in moving bit forward in this research. When we have taken students as sample, we were concentrating only to a category of questions related to student's psychology.

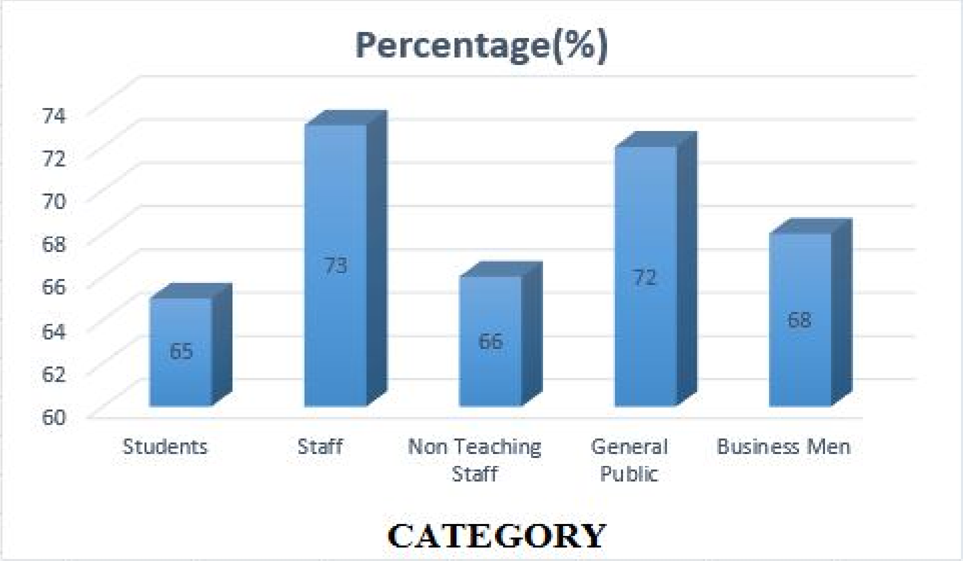


Fig 2. Chart showing results for various categories

Moving further in this we concentrated on co-staff members and started preparing questionnaires for them. This time the questionnaire was much deeper into the psychology aspects and tried to improve the success rate from 65%. As planned we gave a list of questions and asked them to answer. Few days later gave a simple question and asked them to answer so as to take this as a login process. This time there was an increase in the success rate from 65% to 73% i.e. 73%of the staff member's answers were matching with what we expected.

IV. CONCLUSION

In this way we think this might be useful in safe guarding the user's accounts. This may be a trial in finding a solution for password free authentication. Overall, we can hope for a world where there won't be any scope for remembering our passwords.

This proposal if applied with much more psychology professionals and experts in preparing the questionnaire will give us a good result in analysing a person. Even if the result obtained is 10% positive in authentication process, we think this 10% can be improved on taking experts advice and can serve our purpose. Based on this analysis we are trying to develop a software by the final year students and apply this in the intranet used in our college.

REFERENCES

[1].Vipul Sharma, Sunny Kumar, "A New Approach to Hide Text in Images Using Steganography"-*International Journal of Advanced Research in Computer Science and Software Engineering*-Volume 3, Issue 4, April 2013-ISSN: 2277 128X

[2].Kelly D Lewis, James E Lewis, "Web single sign-on authentication using SAML", International Journal of Computer Science Issues, ISSN: 1694-0784, Vol. 2, 2009, PP 41-48.

[3].Wazir Zada Khan, Mohammed Y Aalsalem, Yang Xiang, "A Graphical password based system for small mobile devices", International Journal of Computer Science Issues, e-ISSN: 1694-0814, Vol. 8, Issue 5.

[4].Smita. S., Mudholkar, Pradnya. M. Shende, Milind V Sarode, "Biometrics authentication technique for intrusion detection systems using finger print recognition", International Journal of Computer Science, Engineering and Information Technology, Volume 2, No. 1, February 2001, PP 57-65.

[5].M. Sreelatha, M. Shashi, M. Anirudh, MD. Sultan Ahamer, V. Manoj Kumar, "Authentication schemes for session passwords using color and images", International Journal of Network Security and its applications, Vol. 3, No. 3, May 2011, PP 111-119.