International Journal on Recent Researches In Science, Engineering & Technology

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.

Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 4, Issue 8, August 2016.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

VIRTUAL PASSWORD SCHEME USING ANDROID HELPER APPLICATION

P.Sathish Kumar[1], BimalKalsa[1], P.Rama[1], Prabhakarran[2], P. K. Prakasha[2]

[1]Assistant Professor, Department of CSE, Loyola Institute of Technology, Chennai.
[2]Associate Professor, Department of CSE, Loyola Institute of Technology, Chennai.
[3]Professor, Department of CSE, Loyola Institute of Technology, Chennai.
Corresponding Author : Email: psathish92@gmail.com

ABSTRACT:

Today, The Internet has entered into our daily lives as more and more services have been moved online. Most current commercial websites will ask their users to input their user credentials for authentication which can be stolen. Many schemes, protocols and software have been designed to prevent users from some specified attacks. In this paper, a password protection scheme that involves a small amount of computing done by an helper application, which will be resistant to phishing scams, Trojan horses, and attacks by using either secret little functions or virtual passwords instead of the traditional system. The main disadvantage of the One Time Password is stolen-verifier attack; an attacker who has stolen user verifiers from the server can impersonate legitimate users and theft attack; an attacker who has stolen the server's secret can impersonate legitimate users whereas in our proposed system these can be overcome as some additional computation has to be done thereby preventing above mentioned attacks and our system uses advanced mechanism called as Virtual Password .A helper application ensures that the user’s workload is reduced by performing additional computation.

KEYWORD: One Time Password, Generator Key, Helper Application, Social Engineering Attacks, VirtualPassword Scheme, µTESLA Authentication.

1. INTRODUCTION

Internet which is a major part of every human's life helps one to do work easily and efficiently but its security is always questioned. Some of the very important processes done by the users include banking, checking E-mail and many more which contains very sensitive data. A big question arises in everyone’s mind whether our data is safe since all financial, personal, confidential data can be stolen by adversaries/hackers. An online environment is safe if and only if the security is tightened by using various security algorithms.

Some of the ways a hacker or adversaries uses to find out valuable data includes Phishing, key-loggers, Shoulder surfing which are termed as Social Engineering attacks. Hackers also use the hard way of decoding the password such as dictionary attacks as well but it takes a lot of time than the previous mentioned methods. In order to overcome all the above mentioned attacks many algorithms and methods are used among which one powerful mechanism is Virtual Password Scheme. Social Engineering is a big tool used for compromising security which is done usually by exploiting the trust of the user and knowing the valuable data. Hackers or adversaries trick the users into giving them the passwords or other information which is of high value. Some of the various social engineering attacks are as follows

- Phishing
- Pretexting

- Tailgating
- Shoulder surfing
- Trojan

PHISHING:

Phishing is a power tool to obtain very sensitive information from the people who are very new to the internet. It is a fraudulent practice of obtaining information such as passwords credit card numbers by sending emails about a lottery won by a targeted user which can be collected by sending some key personal information. Phishing has proved to be a easy and effective way of obtaining sensitive data from the people.

PRETEXTING:

Pretexting which has increased in the recent past focuses on creating a good fabricated scenario or a pretext which they use to steal their victims password and sensitive data. These attacks mostly are carried out over a period of time by gaining trust from the victim.

TAILGATING:

Tailgating does not work in very big companies whereas it's most suitable for smaller organizations, where the intruder enters the building when an employee uses his/her card for entering restricted area. Tailgating has to be stopped in order to save the servers from intruders who collect information for unethical purposes.

SHOULDER SURFING:

Shoulder surfing is an effective way of gaining information such as ATM PINS or banking user names and passwords. Shoulder surfing can be overcome using another level of security which in this paper is virtual functions using android helper application.

TROJAN:

Trojan which refers to a set of code which obtains the key information which are entered in the computer which includes various passwords for different email accounts or even the bank passwords. This can be reduced only by installing proper anti-virus software's and also not by using non-certified products which definitely contains malicious codes. Trojan also acts like a key-logger, which collects all the data typed and sends it to different computers where the intruder/hacker/adversaries need them to be.

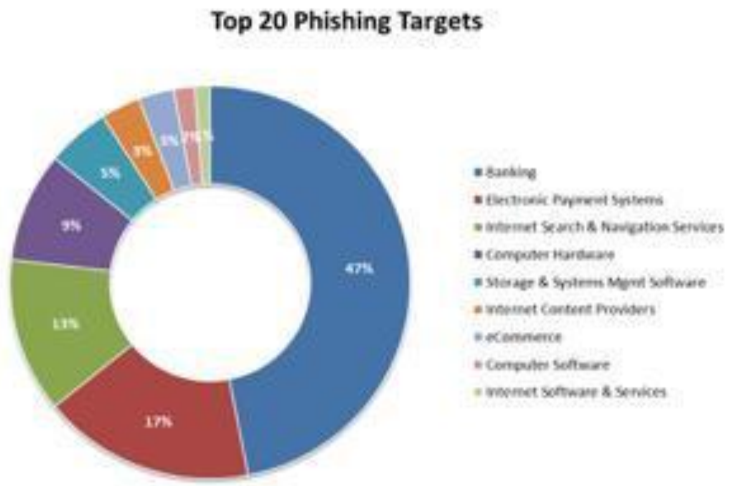


Fig 1: Top 20 Phishing targets

2. RELATED WORK

2.1SMS-BasedOne-Time

Passwords:

This paper takes an in-depth view of OTP authentication and its decline as a strong security measure. Attacks against OTP schemes such as cellular network insecurities, design issues in the mobile phone at hand are a sample of the attacks that can reduce the strength of the OTP scheme are listed. Methods of defending against the proposed attacks are also detailed, which include end to-end encryption on the SMS channels, dedicated channels for OTP and so on. All forms of protection against the attacks have been implemented and the effectiveness of the measures have been studied.

Advantages: Lists protection measures againstattacks that could compromise OTP schemes, and their implementation.

Disadvantages: Does not improve upon the actualOTP scheme. Only security against the flaws in the scheme itself.

2.2 Phishing and Anti-Phishing Techniques:

This paper covers a brief description of what phishing means, a basic classification of the types of commonly used phishing techniques by attackers, and a basic list of things to be done to prevent phishing. A best practices list specifies how phishing can be prevented. Also the role of bot nets in phishing is also explained in detail along with surveys of users regarding phishing.

Advantages: A detailed analysis of phishing and itsmethods of execution are clearly explained in detail.

Disadvantages: No methods on how to actuallyprevent any of the listed attacks is specified in this paper.

2.3 Virtual password using random linear functions for on-line services, ATMs, and pervasive computing:

This paper provides a novel method by which a password can be computed by a user using a mathematical function, in this case, a random linear function. The method in which this is implemented, a helper application which can be used in the computation of this virtual function, an implementation of an early version of a virtual password scheme is detailed in this paper.

Advantages: An early implementation of virtualpassword scheme which can improve upon conventional password security and strengthen it.

Disadvantages: A more detailed analysis on thefunctions used and complexity of the function is not specified.

3. PROPOSED SYSTEM

To improve authentication security to a greater level than currently existing schemes, we propose the use of an authentication scheme with a greater chance of being resistant to the previously mentioned attacks, known as Virtual Password Scheme. Unlike the traditional way, a small amount of computing is required to be performed to obtain the actual password, which in turn is presented to the system for successful authentication.

A virtual password is nothing more than a dynamic password. Each time a dynamic password is generated which is based on a predefined “Password scheme”. This, in principle, prevents any sort of phishing attack or key loggers from succeeding, As even if the password captured by these tools, it would be different the next time the attacker tries to log in to the system with the captured credentials. A final and major part of our proposed project is to make the scheme used here as user-friendly as possible, by creating a Virtual Password Helper Application, which can be used on a user’s personal mobile computing device, to aid in the calculation of the virtual password, thus providing added security in the form of the user’s device, as in the case of the commonly used One Time Passwords. The Helper application would run the secret functions used on the salt provided by the user and thus generate the virtual password thus reducing the burden on the User’s part.

4. MODULE DESCRIPTION

The complete system is comprised of two major parts: The server side of the authentication system and the helper application, which is the user's computing device for calculation of the actual password from the salt. The server side is comprised of the login module, where the user is authenticated and the salt is generated, the signup module ,where a new user is created and logged into the system and the virtual functions ,which are the core of the system as they completely define the levels of security of the user's password also.

On the client side is the helper application, which helps in calculating the actual password from the selected virtual password scheme, which is decided during the signup module phase.

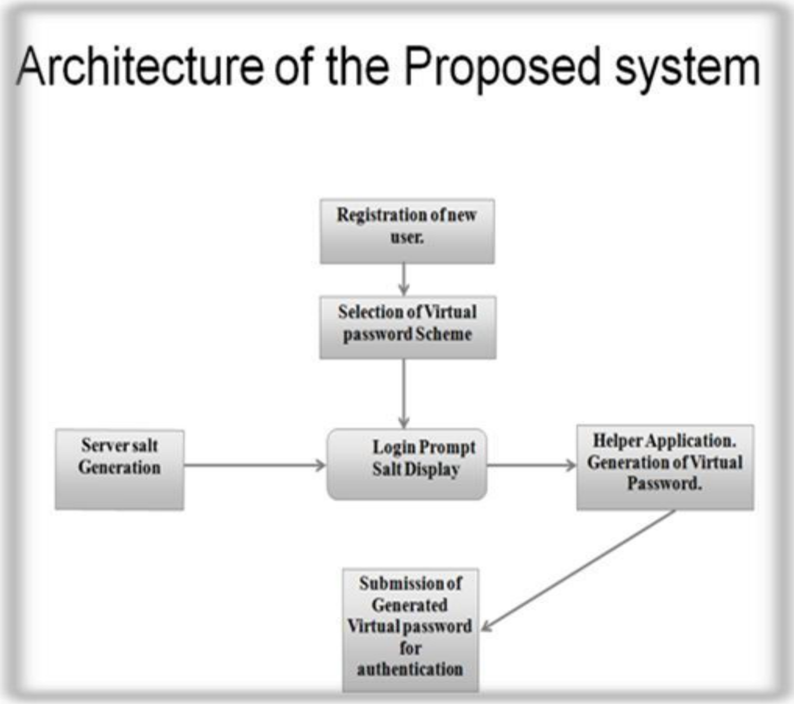

Architecture of the Proposed system
Registration of new user.
Selection of Virtual password Scheme
Server salt Generation
Login Prompt Salt Display
Helper Application. Generation of Virtual Password.
Submission of Generated Virtual password for authentication

Fig 3 Proposed System

4.1 LOGIN MODULE:

1. This module is used to obtain the generated key and the password.
2. The user enters the username in the username textbox and clicks the submit username button.
3. If the username is invalid, the system throws the invalid username error.
4. If the username is valid, the generated key field gets populated with the generated key that's unique to that user.
5. The user enters this generated key in the android helper application and selects the function that was selected during registration.
6. The generated password is displayed in the android helper application.
7. The user then enters this password in the password textbox of the login module and clicks on the submit password button.
8. If the password entered is valid, the log in attempt is successful.

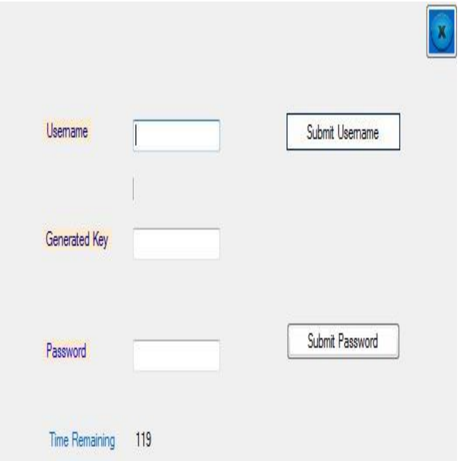


Fig 4.1 login module

4.2 SIGNUP MODULE:

1. The sign-up module is used to register a user in the system.
2. The user fills the details in the form and selects the preferred virtual function from the list of six functions.
3. The users can also enter their own function in the custom virtual function text box.
4 .The user then clicks on the Sign-up button and the registration is successful.
5. The user enters this username during Log in.

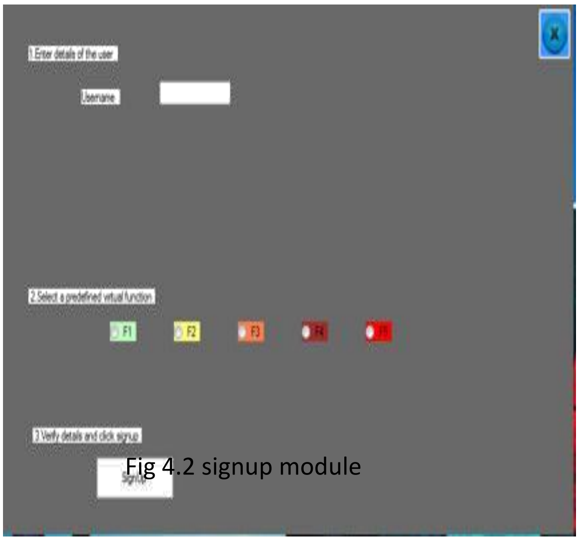

1.Enter details of the user
Username
2.Select a predefined virtual function
F1
F2
F3
F4
F5
3.Verify details and click signup
Signup

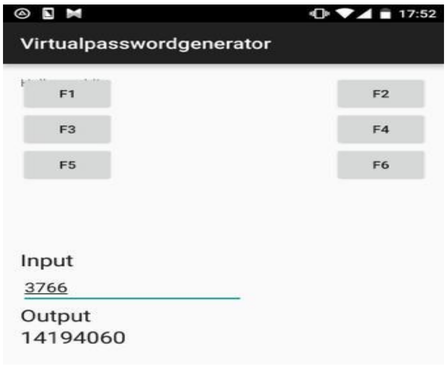
Fig 4.2 signup module

4.3 VIRTUAL FUNCTIONS

1. The six selected functions contain difficulty level from easy to hard which can be selected as per the needs of the user.
2. The mathematical functions are calculated both at the server end and also by the helper application using the random generated number.
3. The random generated number is unique for all users.
4. Users can also specific their own virtual functions during Sign-up.
5. Password theft can be decreased to a larger amount by the use of complicated virtual password functions for very sensitive data.

4.4 ANDROID HELPER APPLICATION

1. This android helper application contains various functions mentioned during the registration process.
2. The user has to enter the generated key into the input field and select the appropriate function.
3. The helper application calculates the password itself and displays the password in output field
4. The password generated is entered in the log in page.
5. Log in is successful if the password entered is correct.



Input
3766
Output
14194060

Fig 4.4 Android Helper Application

5. VIRTUAL FUNCTION

In this section, we propose examples of virtual functions and analyze how they secure a user password. However, our proposed approach is not limited by these examples. We consider digits here as an example, but our scheme is not limited in the number of digits, nor is it even limited to using only digits.

5.1 EARLY ATTEMPTS:

In the beginning we pursued objective functions as virtual functions since we thought that since bijective functions had reverse functions, it was easy to verify a user by the server. Later, we believed that it was not necessary for virtual functions to be bijective, but injective. We began by using simple operators, such as plus or minus some secret value,

e.g., $B(x) = (x+a) \bmod Z$, ----- (1)

Which is easy to use, where x is the fixed part of the user's virtual password and a, is the secret value. We immediately excluded this case of equation (1), since it is easy to attack and violates the first requirement that is, it has no random variable. We concluded that we could use a simple linear function that includes a random variable, such as

$B(x) = (a*x+y) \bmod Z$, ----- (2)

Where x is the fixed part of the user's virtual password, y is a random number the system provides to the user in each login session and a, is kept as secret. This function (2) involves the random factor, but it violates the unobservable rule. This is because once the adversary obtains the function output k and random factor y (through shoulder-surfing or Phishing), they can easily login to the system based on the stolen information. This is because with k and y, they can deduce (a*x) mod Z = (k-y) mod Z. Then the adversary can log in to the system with (a*x +y') mod Z, Where y' is a new random number. Then, we considered the function

$B(xi) = axi+yi \bmod Z$, ---- (3)

Where xi is one digit of the password, yi is a random number provided by the server, and a, is kept as secret. However, we discovered that this function is subject to shoulder-surfing attacks. For example, if a hidden camera records a user's activity, then it is easy to obtain axi if yi is known. For example, suppose that you have a virtual password 123 and the function (3*x + y) mod 10. In the login session, the system provides the random number, 456. You Calculate, (3*1+4) mod 10=7, (3*2 +5) mod 10=1, and (3*3 +6) mod 10=5, So that it is 715. Once the adversary steals the random number and the dynamic password the user input, the adversary can determine 3*x1 = 3, since (7-4) mod 10=3, 3*x2 = 6 since (1-5) mod 10=6, and 3*x3 = 9 since (5-6) mod 10=9. Now, the adversary is able to access the system. If the system generated random number is 789, the adversary can enter the system by providing the password 048, where 0= (7 + (7-4)) mod 10, 4 = (1+ (8-5)) mod 10, and 8 = (5 + (9-6)) mod 10. This is the correct real password.

5.2 FURTHER ATTEMPTS:

Next, we added a constant factor to the linear function:

B x a x y c Z ( ) ( ) mod i i i = + + [ ] ---- (4)

Where a and Z are relatively prime, xi is one digit from the fixed part of the user's virtual password, yi is one random digit provided by the system, and a and c are the constant factors of the linear function, which the user has to remember. The B (xi) is a bijective function if and only if gcd (a, Z) =1 [26] Where gcd denotes the Greatest Common Divider function. In fact, we can prove that this function can withstand Phishing, key logger, and shoulder surfing attacks by the follow security analysis. Let x1x2…xn and [a(xi+yi)+c] mod Z denotes the user's fixed password, and the virtual password, respectively, where y=y1y2..yn is random number provided by the system/server.

6. RESULTS AND SURVEY

In order to estimate the efficiency along with the usability of our system we conducted a survey by making people use the system along with the helper application for logging in. In our testing, each volunteer was asked to try to log in to our test website for two rounds. For the first round, they needed to calculate the password by themselves, and for the second round, they used a helper application to calculate the password for them. They completed each round ten times and recorded the time it took them to complete their log in.

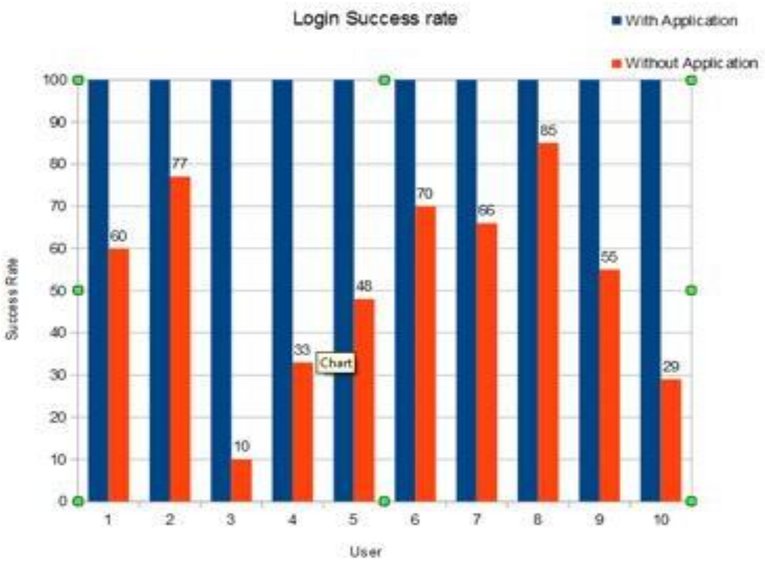


Fig 6.1 Login Success Rate

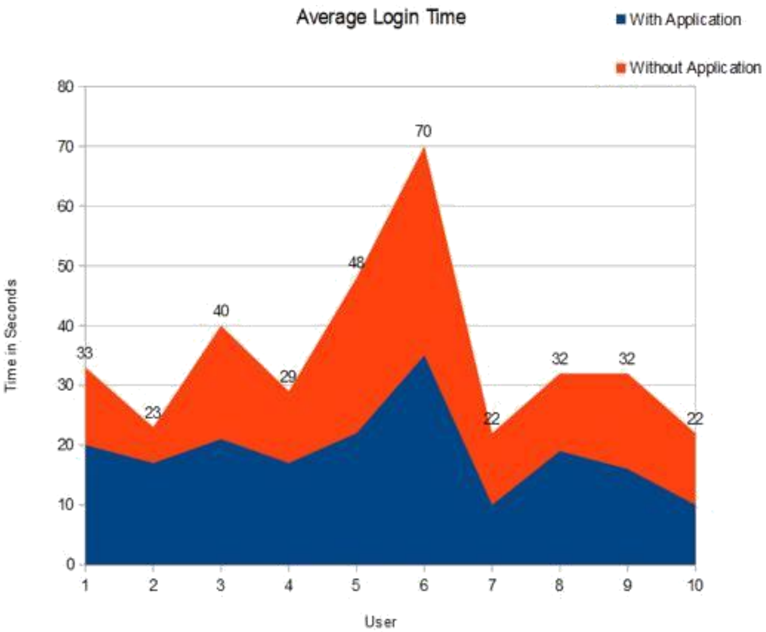


Fig 6.2 Average Login Time

From the figure 6.3 it is clear that most of the users were happy with the usage of helper-application which reduced the log in time.

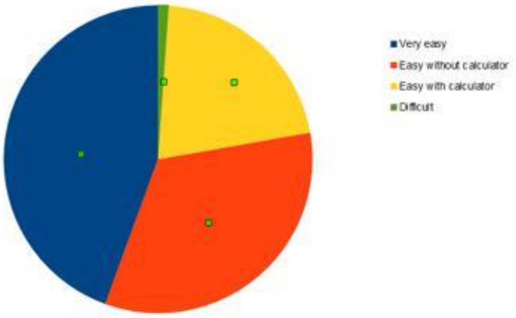


Fig 6.3 Survey on usage of helper-application

We also conducted a survey which helped us find most of the users had no idea of how to stop these social engineering attacks, mainly Phishing and Key-loggers which is depicted in the form of pie chart. We also found out that people felt easy to complete single digit calculations. In our proposed even though user can choose very hard virtual functions, helper-application is used to solve. From the survey, it is evident most of the users felt single digit calculations were very easy. Only one percent of the total users felt calculating as a difficult task.

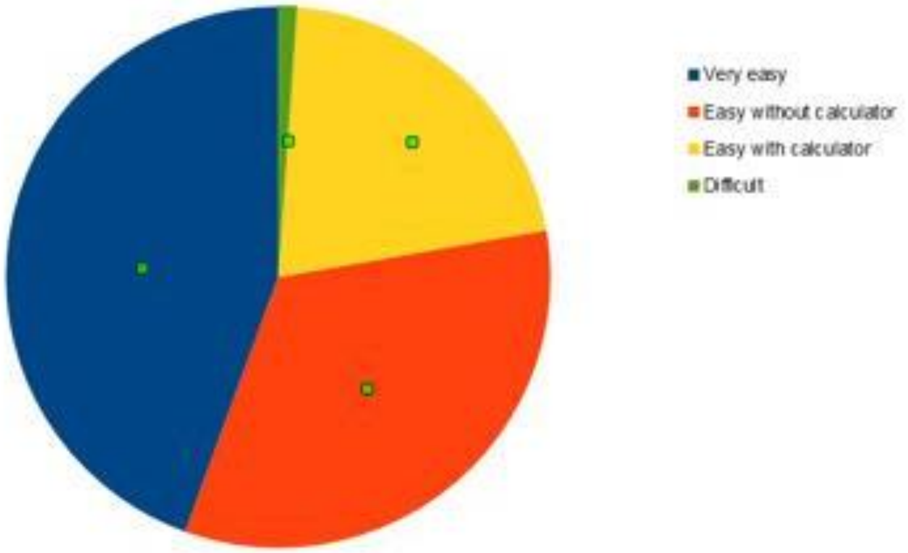


Fig 6.4 Single Digit Calculation Survey

Given below our survey of users, regarding their knowledge of key logging attacks and how to defend against it. Reports show that over 50% of the users are completely unaware of such attacks let alone how to defend against it. 30% of users are aware of such attacks but are ignorant of ways to defend against it. Only a very small percentage of our users have both heard and know of ways to defend against such attacks.

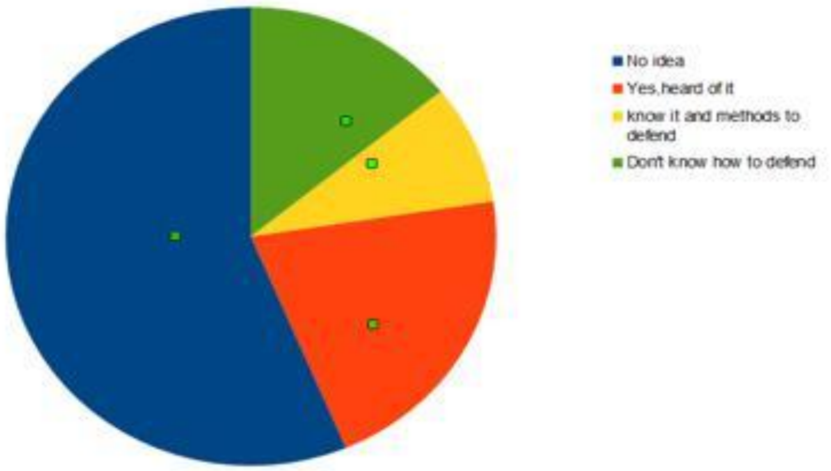


Fig 6.5 Key logger Survey

Given below our survey of users, regarding their knowledge of Phishing attacks and how to defend against it. Reports shows that over 50% of the users are completely unaware of such attacks let alone how to defend against it. 30% of users are aware of such attacks but are ignorant of ways to defend against it. Only a very small percentage of our users have both heard and know of ways to defend against such attacks.

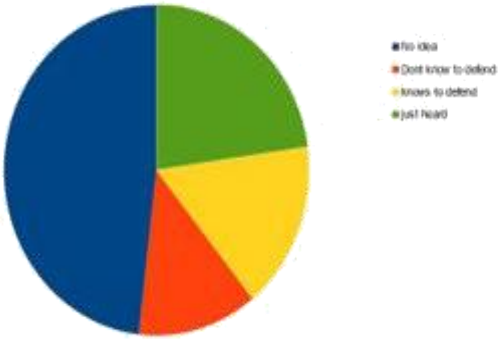


Fig 6.6 Phishing Survey

Yet another survey was conducted on the willingness of the users to change from their default password schemes to the virtual password scheme suggested here. Thus the complexity of the password scheme is the major factor in deciding whether the users will adopt a more secure scheme as opposed to their old ones.

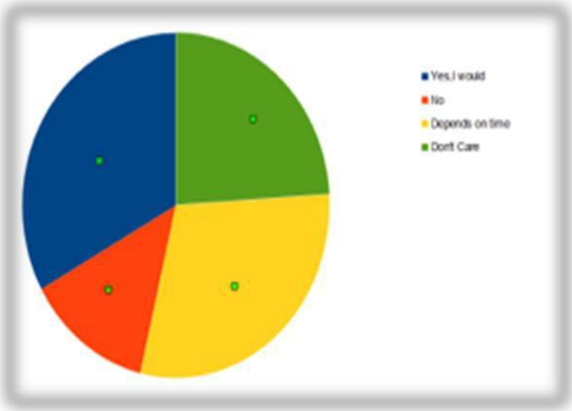


Fig 6.7 User Survey

7. CONCLUSION

In this paper, various methods which were used for stealing passwords by adversaries/Hackers were address and also how to overcome them. Our proposed virtual password scheme using android helper-application helps the users to secure their passwords in online transactions with the help of virtual functions whose calculations are done by the helper application only thereby reducing the burden on the users. Our Tests and surveys indicate the use of the proposed system. No security system is fool proof which means with intensive and intelligent virtual functions we can safeguard our accounts in this online environment easily.

8. FUTURE WORK

In future we have planned to improve the system by adding complex functions and also including algorithms which counters social engineering attacks as well as other attacks. IN future we have planned to use alphanumeric salt generation.

REFERENCES

[1] M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li,“Virtual password using random linear functions for on-line services, ATMs, and pervasive computing,” Compute. Common.J. Elsevier, vol. 31, no. 18, pp. 4367–4375, Dec. 2008

[2] J. M. McCune, A. Perrig, and M. K. Reiter, “Seeing-is-believing: Using camera phones for human-verifiable authentication,” Int.J.SecurityNetw., vol. 4, nos. 1–2, pp. 43–56, 2009.

[3] V. A. Brennen, "Cryptography Dictionary," vol. 2005, 1.0.0ed, 2004.