JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SURVEY ON THREE STEP AUTHENTICATION SYSTEM FOR DESKTOP APPLICATIONS

[1] Siddhesh Deepak Patil, [2] Dr. Umarani Chellapandy

[1] Student, School of Computer Science and Information Technology
[2] Associate Professor, School of Computer Science and Information Technology
Jain Deemed-to-be University, Bangalore, Karnataka

Abstract: - Authentication, security, and confidentiality are a number of the foremost important topics of cyber security. There are many solutions presented to users for strengthening the safety of login password-based authentication methods. Primarily this has been through the utilization of two-factor authentication methods. Two-factor authentication is that the combination of two single factor authentication mechanisms. The focus of this research is to address and analyze the implications of using three-factor authentication model for added security in windows application, websites and mobile apps. This paper will present a windows application we created which could provide a potential method for three-factor authentication.

Keywords: - Authentication, One Time Password, Three-Factor Authentication, Image Based Password.

Introduction

Authentication it can be said as a process of verifying the identity of the user.

Three-factor authentication means adding up another one layer of verification to the two-factor authentication (i.e., password + OTP) to increase the assurance that the bearer has been authorized to access secure system. The first layer of this application consists of user id or email id with password, the unique of this password is that it has its own password encrypting method. It has its own way of entering the password, even which is unique in its own way. Second layer of this application is One Time Password system with 6-digit number which can be sent to the email address or to phone number. Third and final step is to select the right image from a set of images, the right image will be sent to the email address. Once completing all these steps, you will be able to access the system or application. This application also has a virus remover feature which removes files which are possibly a virus or virus shortcut, this also has login time face capture which takes photo of person who tries to login the system it doesn’t matter whether the user has entered right password or wrong

Literature Review

Most of the authentication mechanisms are solely based on password. Password are vulnerable as they use same passwords many times and don’t change them at regular basis, usually they are short string of characters and poorly selected. They can be easily cracked by simple dictionary attacks, to avoid these things multi-factor authentication helps to secure it.

In [1], Ewe Syta. has different authentication methods that can be used, they are Knowledge-based (Numeric, Alpha-numeric, Graphical password), Possession-based (Token) and Biometric-based (Fingerprint, Facial recognition, Iris recognition, Hand geometry). It has explained an approach that users taken-based authentication which is cost effective, easy to use and secure. It has some security issues like RFID technology’s nature is contactless, dues to this anyone can read the passive tags if they are on the same frequency.

In [2], Fujii H. has expressed view on two-step authentication using SMS or Voice call to prevent phishing attack. It has descried about two different methods, two-authentication using SMS and voiceprint response (SV-2FA) and SV-2FA/Certificate Provisioning by using net banking model.

In [3], G. E Blonder. Has proposed graphical password technique for first time, it suggest the technique that the user is required to point one or more predetermined position on the image, which he selects during registration time for every login. As compared to 4-digit PIN which has the combination of 10,000 possible but in graphical password using three taps its correct order there can be over 13.6 million possible combinations.

In [5], Rane, in this new approach, images are shown to users during login phase. The user chooses several images in order to select a password. After this, the user selects one image and clicks to draw the secret. When logging in, the user draws the secret that was in the registration phase. Sequence of clicks is not required.

In [6], Nagesh, this paper is a unique and esoteric study about using patterns as passwords and developing an extremely secure system employing 3 levels of security (Text Password, Pattern-Lock, and One-Time automated generated password).

Terminologies

Authentication: - Authentication is the verification of someone's identity or that of something. The authenticator uses the information provided to determine if someone or something is who they claim to be or what they claim to be. It is also the technology provides access control for system by checking to see is a user’s credentials match the credentials which he/she given during the time of creating the account which are stored in the database. There are three type of authentication which can be defined

Single-Factor Authentication: - These are the basic way of authentication with minimal security, it only requires only User ID and password to login.

Two-Factor Authentication: - In this the authentication has two layers first one will be with User ID and Password and the second layer can be biometric or One-time Password.

Multifactor Authentication: - In this there will be more then two layers of authentication i.e., minimum of three steps or above. Which can be like this first step will be User ID and password, second step will be using One-time password which can be sent to either mobile number or Email ID, the third step may be of biometrics like facial scan, fingerprint or Iris scanner. We can add up more step to the authentication as required like Retina recognition, Face recognition, DNA matching, Signature recognition, Voice recognition..., and many more steps can be formed as required.

One-time Password: - A One-time password is a randomly generated number or alphanumeric code which may be in minimum digit of 4 to maximum of 8 and they have a time limit of 30 seconds to 60 seconds. It is used to authenticate the user’s identity weather it is the same person or not. If someone tries to use our account and we have enabled One-time password it will be difficulty for them to use as an OTP as it will be sent to the register mobile number and will have a certain time limit after that it will be useless or have to create a new one.

Picture OTP: - It is picture or photo One-time password it is same as the OTP, but with different working. The working of this is like the user will be shown a set a photo displayed on the screen (they can be 4 to 8 photos) from which he has to select the right one, the right image will be sent to his email-id from where the user has to see and select the right image, even this has a certain time limit which can be from 0.1 to 2 minutes depends upon the developer of that project using it for, as it takes time to receive the mail so it has a time limit of 2 minute.

Antivirus: - Basically an antivirus is a software which protects and detect a devices from harmful virus, malware. It keeps the system protected from the virus and it will be working all the time from the start of the system till it is turned offed. It scans the whole system to see any malicious file or code, if it finds any it will delete that particular file before it would harm the system.

Login time face Capture: -This is a new type of approach used for security of the application, whenever the user or someone else tries to login the system it takes the picture of that particular person and stores it the application. Through this the user will have the details and photo of that person who tried to login the system without his knowledge. For working of this feature camera is must required on the system.

Conclusion

In this paper there is a new approach of implementing password with the very unique login methodology that will trick the intruders who are trying to copy your password and also capture the picture if the user tries to crack the password. As there is use of one-time password it is tough to crack it. The other features in guard we can discuss are Test Anti-Virus and remove the shortcut virus etc. these may be helpful for most of the systems.

References

[1] Syta, E., Kurkovsky, S., Casano, B. RFID-based authentication middleware for mobile devices. Proceedings 43rd Annual Hawaii International Conference on System Sciences (HICSS '10), January 2010

[2] Fujii, H. and Tsuruoka, Y. SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge Response. Proceeding's 8th International Conference for Internet Technology and Secured Transactions (ICITST -2013), IEEE, 2013, pp. 283-287

[3] G. E. Blonder, "Graphical Password," US5559961 A, Lucent Technologies, Inc. (Murray Hill, NJ), Sep. 1996.

[4] Gehringer, Edward. (2002). Choosing passwords: Security and human factors. International Symposium on Technology and Society. 369 - 373. 10.1109/ISTAS.2002.1013839.

[5] Rane, Pratibha & Shaikh, Nilam & Modak, Prarthana. (2016). Secure Authentication Using Click Draw Based Graphical Password Scheme. International Journal of Advanced Engineering Research and Science. 4. 1-4. 10.22161/ijaers.4.1.1.

[6] Nagesh.D Kamble, J.Dharani. Implementation of Security System Using 3-Level Authentication