MULTIFACTOR AUTHENTICATION FOR E-COMMERCE APPLICATIONS

Namita Redkar, Manish Yadav, Prof. D.R. Ingle
Computer Department
Bharati Vidyapeeth College Of Engineering
Navi-Mumbai,India
Namita.redkar@gmail.com
Manishyaday733@gmail.com
dringleus@yahoo.com

***Abstract*—we are going to implement 3D password for online website. We are going to implement this project using PHP, MYSQL and CopperLicht. In this project there are three stages. In first stage of security user need to provide his username and password, if username and password given by user is correct then user will enter in 3D environment. 3D environment is the second stage of security, in this user will move some objects and those locations of objects will be taken as password, if the graphical password is correct then user will get one time generated code on his mobile. This is final third stage of security, then user need to enter that to our interface and if entered code is correct then user's transaction will be successfully completed.**

Keywords— 3D password, security for e-commerce applications, multifactor authentication

I. INTRODUCTION

In e-commerce applications authentication is require to prove the Identity of buyer or seller. In online banking application user get authenticated with the help of passwords only. Is this system so secure to trust? [12][16]

Password-Based user authentication systems are low cost and easy to use. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access devices he/she employs. A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access. Authentication describes the process of positively identifying potential network users. The result of the authentication process is the basis for permitting or denying further actions. An authentication process consists of three stages: access request, information extraction and authentication. The conventional authentication system depends purely on textual user name and password. It uses Prefixed information which is stored as a valid user identity in database. Textual based authentication system remains dominant technique currently. There are several possible factors for determining the authenticity of a person, device or system. For example, the test could be something known (e.g., PIN or password), something owned (e.g., key, dongle, or smart card), something physical (e.g., biological characteristic such as a fingerprint or retinal signature), a location (e.g., Global Positioning System location access). In general, there are four human authentication techniques: 1. what you know (knowledge based). 2. What you have (token based). 3 What you are (biometrics). 4. What you recognize (recognition based) [8]. In general, the more factors that are used in the authentication process, the more robust the security process will be. When two or more factors are used, the process is known generically as multi-factor authentication. Security starts with you, the user. Keeping written lists of passwords on scraps of paper, or in a text document on your desktop is unsafe and is easily viewed by prying eyes (both cyber-based and human). Using the same password over and over again across a wide spectrum of systems and websites creates the nightmare scenario where once someone has figured out one password, they have figured out all your passwords and now have access to every part of your life (system, e-mail, retail, financial, work). The strength of a password is related to its length and entropy. The importance of length is fairly obvious. A 4- digit pass code has 10,000 possible values from 0000 to 9999, while an 8-character password has billions of possible values.

Entropy is a measure of the randomness in the password and is equally important. Passwords that use predicable sequences of digits (e.g., "1234") are far easier to predict than more random passwords. Unfortunately, the greatest weakness in the use of passwords is that users tend to pick passwords that are easy to remember and thereby have very low entropy and are easy to predict. Another weakness is the ease of third party eavesdropping. Passwords typed at a keypad are easily observed or especially in areas where attackers could plant wireless cameras or hardware keystroke sniffers. Key loggers capture keystrokes and store them somewhere in the machine, or send them back to the adversary. Shoulder surfing is a well-known method of stealing other's passwords and other sensitive personal information by looking over victims' shoulders while they are sitting in front of terminals or in front of an ATM machine [3][2]. This paper presents a new password choice technique. The new technique will be proven secure against shoulder surfing and other form of attacks.

All e-commerce environments require support for security properties such as authentication, authorization, data confidentiality, and non - repudiation. The most common method of authentication or protection against intrusion in a computer system is to use alphanumeric usernames and password. [14][17]Choosing a strong password and protecting the chosen password has always been a popular topic among security researchers. Studies reveal that users today have on an average approximately 15 passwords – protected accounts. [5][11] One password may be easy to remember, but handling many passwords is time-consuming task and a security hazard. Every forgotten or lost password results in significant cost. Passwords are not secured at all as they can be guess they can be stolen. To overcome weakness of passwords we need stronger authentication solutions. Till date many techniques are proposed for protecting the passwords and tried to eliminate password hacking problem. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. In this paper, we present and evaluate our contribution, on the multifactor authentication technique. We tried to enhance the security by using multifactor authentication. In which two three factors are taken in to consideration.

II. IMPORTANCE OF AUTHENTICATION

Security decision-makers in November and December 2008, Forrester found that [1] [9]:

1. Authentication is a key to gaining customer trust, although providing secure authentication is a daunting process.

Businesses are faced with a large volume of Web site hits for which authentication is necessary. Seventy percent of those surveyed report that their current authentication methods directly influence their customers' perception of trust. Needing to provide secure authentication in an environment with increasing regulations, rising online fraud, and escalating costs creates challenges for companies that see customer trust as a business priority.

2. Companies understand that upgrades are necessary to provide truly secure authentication and are exploring authentication-as-a-service.

Seventy- five percent of organizations surveyed have budgeted for or are considering an upgrade to their current authentication process or technology within the next year. The survey also found that many line-of- business owners and C-level executives will be involved with this decision-making process. Given their focus on maintaining customer trust, it is not surprising that these business managers will be most interested in the level of customer privacy and the reputation of the service provider.

Authentication Factors [8][10]:

1. Knowledge factors: "something the user knows"
Knowledge factors is the most common form of authentication used. In this form user is required to prove the knowledge of a secret in order to authenticate.

Password: password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on password as one factor of authentication.

PIN: personal identification number (PIN) is a secret numeric password and used in ATMs typically

Pattern: Pattern is a sequence of cells in an array that is used for authenticating the users. E.g. Pattern based authentication is used in Android devices.

2. Possession factors: "something the user has" Possession factors have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession-factor authentication in computer systems.

Soft tokens: The functionality of any disconnected token can be emulated as a "soft token" on a PC or smartphone using deployed software, whereupon that device itself becomes the possession factor. This saves on deployment costs, but against that, the secret is vulnerable to any attacker or malware that can gain full access to the device. The Zeus Trojan, which can now infect mobile devices running Android or BlackBerry OS, specifically targets[9] banking credentials and may forward them to the attacker at a website set up for the purpose, or by SMS messaging. Note: Soft tokens are fundamentally different from virtual token MFA in that "soft" tokens require the user to install software, while virtual token MFA does not.

One-time pads: A one-time pad is a password used only once. Schemes based on a one time pad have been described but are rarely deployed due to the need to supply a new password (or 'pad') for each authentication. Schemes which use a grid-card are not one-time pads, and are akin to requesting a selection of characters from a password *known* by the user (albeit a password written down). As such, they only protect against re-play attacks (as the same selection of characters can't be sent) and not against duplication of the entire grid (or the building up of a duplicate answer grid over time).

UniOTP*:* UniOTP is an event/time-based one-time password token with robust plastic case. Its dust proof, water proof and anti-broken features ensure it can work under adverse circumstances, such as construction, military and etc. By clicking the button, the device will display a serial number as the dynamic password.

Mobile phones: There is presently only limited discussion on using wired phones for authentication; most applications focus on use of mobile phones instead.

3. Inherence factors: "something the user is"

Biometrics: A human thumbprint - a common type of biometric data used in authentication. Biometric authentication also satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault. However, while this type of authentication is suitable in limited applications, this solution may become unacceptably slow and comparatively expensive when a large number of users are involved. In addition, it is extremely vulnerable to a replay attack: once the biometric information is compromised, it may easily be replayed unless the reader is completely secure and guarded. Finally, there is great user resistance to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes. In short, selection and successful deployment of a biometric authentication system needs careful consideration of many factors.

III. 3-D ENVIROMENT

The 3-D password [7] is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. It is the user's choice to select which type of authentication techniques will be part of their 3-D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user simply avoids interacting with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large number of objects and items in the environment, the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password.

CopperLicht[16] is a JavaScript library/API for creating games and interactive 3D applications using WebGL, developed by Ambiera. The aim of the library is to provide an API for making it easier developing 3D content for the web.

IV. ONE-TIME PASSWORD

A **one-time password** (OTP) is a password that is valid for only one login session or transaction.[16][17] OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that, if a potential intruder manages to record an OTP that was already used to log into a service or to conduct a transaction; he or she will not be able to abuse it since it will be no longer valid.

In OTP password generation, now a days as per the survey individual's perspective there is a necessity to have a mobile phone that bring ease in his day to day activities hence by taking this thing into consideration third level of security i.e. OTP generation has been implemented .Due to this instant passwords user can trust this application while performing online transactions.

OTP generation algorithms typically make use of randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

1. Time-synchronized

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source. An example of time-synchronized OTP standard is TOTP.

2. Mathematical algorithms

Each new OTP may be created from the past OTPs used. An example of this type of algorithm, credited to Leslie Lamport, uses a one-way function (call it f). The one-time password system works by starting with an initial seed s, then generating passwords

$$f(s),\ f(f(s)),\ f(f(f(s))),\ \ldots$$

as many times as necessary. If an indefinite series of passwords is wanted, a new seed value can be chosen after the set for s is exhausted. Each password is then dispensed in reverse, with $f(f(\ldots f(s))\ldots)$ first, to $f(s)$.

If an intruder happens to see a one-time password, he may have access for one time period or login, but it becomes useless once that period expires. To get the next password in the series from the previous passwords, one needs to find a way of calculating the inverse function f^{-1}. Since f was chosen to be one-way, this is extremely difficult to do. If f is a cryptographic hash function, which is generally the case, it is (so far as is known) a computationally infeasible task.

In some mathematical algorithm schemes, it is possible for the user to provide the server with a static key for use as an encryption key, by only sending a one-time password.

One-time passwords will require a user to provide a response to a challenge. For example, this can be done by inputting the value that the token has generated into the token itself. To avoid duplicates, an additional counter is usually involved, so if one happens to get the same challenge twice, this still results in different one-time passwords. However, the computation does not usually involve the previous one-time password; that is, usually this or another algorithm is used, rather than using both algorithms.

The methods of delivering the OTP which are *token-based* may use either of these types of algorithm instead of time-synchronization.

V. PROPOSED SYSTEM

The proposed system is a multi-factor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user's freedom of selection is important. The following requirements are satisfied in the proposed scheme:-

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.

3. The new scheme provides secrets that can be easily revoked or changed.

ALGORITHM DEVELOPMENT

1. Start.
2. User opens login page.

2.1 If registered user
then
{
2.1.1. Accept username and password from user.
2.1.2. Convert password to MD5.
2.1.3. If new MD5=MD5 stored in database
Then
{
open 3D interface
else
back to login page.
}
}

2.2 If unregistered user
then
{
2.2.1. Accept username, password and email id.
2.2.2. Convert password to MD5.
2.2.3. Store MD5 in database.
2.2.4. Open 3D environment.
2.2.5. Let user manipulate objects in 3D environment.
2.2.6. Extract x, y, z coordinates.
2.2.7. Store coordinates in database.
2.2.8. Send email alert to user "Registration successful".
}

3. User directed to 3D interface.
   3.1. User manipulates 3D objects.
   3.2. Retrieve x, y, z coordinates.
   3.3. If new coordinates=coordinates stored in database.
   then
   {
   open OTP interface
   else
   back to login page.
   }
4. User directed to OTP interface.
   4.1. User initiates OTP generation.
   4.2. Server generates unique code.
   4.3. Create temporary variable t in server.
   4.4. Unique code=(character array+timestamp)

VI. CONCLUSION

This approach will definitely provide security to the password at less cost, less storage and approximately at same speed as compare to other 3D password techniques. Any user can make use of it no special training is required.

This application is efficient enough to provide a complete security package to perform online banking transaction.

A pictorial representation of password in the second level gives a significant effect of remembering the passwords thereby having less chances of forgetting the password.

Lastly in the third level due to randomize password generation the chances of password getting leak is considerably reduced.

ACKNOWLEDGEMENT

Our sincere thanks to our guide, **Prof. D.R.Ingle** for guiding and correcting various documents with attention and care. He has taken pain to go through the project and make necessary correction as and when needed.

Our heartiest thanks to the project co-coordinator, **Prof. B.W.Balkhande**, for support and guidance.

Our deep sense of gratitude to **Prof. Vidya Chitre**, Head of Department for being our constant spirit of inspiration every now and then.

We express our gratitude to the Principal, **Dr.M.Z.Shaikh**, BHARATI VIDYAPEETH COLLEGE OF ENGINEERING, NAVI MUMBAI, for his support.

We also extend our heartfelt thanks to our family and well-wishers. Lastly, we would express thanks to the team members for their help.

REFERENCES

[1] Improving Security of Ecommerce application, by Using Multifactor Authentication by Anjali S. Yeole VES Institute of Technology. Chembur, Mumbai, India Bandu B. Meshram Professor and Head, Computer Department V.J.T.I, Mumbai.

[2] Fawaz A Alsulaimanand Abdulmotaleb El Saddik, A Novel 3D Graphical Password Schema Multimedia, VECIMS2006–IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems La Coruña-Spain, 10-12 July2006

[3]System Yanjiang Yang,RobertH.Deng, A Practical "Password-Based Two-Server Authentication and Key Exchange "

[4]"Authentication-As–A-Service", A commissioned study conducted by Forrester Consulting on behalf of VeriSign

[5]Khaled Alghathbar, Hanan Mahmoud, Noisy Password Security Technique, *Institute of Electrical and Electronics Engineers*

[6] "Graphical Passwords: A Survey" by XiaoyuanSuo, Ying Zhu and G. Scott. Owen,Department of Computer Science, Georgia State University.
[7]Virtual Realization using 3D Password A. B. Gadicha 1 , V. B. Gadicha 2 , 1,2, Department of Computer Science & Engineering 1,2 P.R.Patil College of Engg & Technology, Amravati, India.
[8] Michael Burrows and Mart´ın Abadi and Roger Needham, A Logic of Authentication, Technical Report 39, Digital Systems Research Center.
[9] Kjell J. Hole and Vebjørn Moen and Thomas Tjøstheim, Case Study: Online Banking Security, IEEE Security and Privacy, Vol. 4, No. 2, pp. 14–20, IEEE Educational Activities Department.
[10] Markus Jakobsson, Steven Myers: Phishing and Counter-measures, 2007, John Wiley & Sons
[11] Fadi Aloul, Syed Zahidi, Two Factor Authentication, Proceedings of the IEEE International Conference on Computer Systems and Applications, pg. 641-644, 2009.
[12] Internet Banking Two-Factor Authentication, Costin Andrei SOARE IT&C Security Master Department of Economic Informatics and Cybernetics Bucharest University of Economic Studies, ROMANIA.
[13] Alecu F., Internet Banking, Informatica Economică, nr. 4 (40), 2006, pp. 104 – 106, ISSN 1453-1305
[14] Anders Moen Hagalisletto, Arne Riiber, Two-factor authentication, Proceedings of the 1st International Workshop on Security for Spontaneous Interaction, IWSSI 2007, Innsbruck, Austria, 2007.
[15] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems,"
IBM systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
[16] A. Bhargav-Spantzel, A.C. Squicciarini, E. Bertino, S. Modi, M. Young, and S.J. Elliott, "Privacy Preserving Multi-Factor Authentication with Biometrics," J. Computer Security, vol. 15, no. 5, pp. 529-560
[17] D.V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proc.Second USENIX Workshop Security.