Improving Security of E- Commerce application by using Multifactor Authentication

Anjali S. Yeole VES
Institute of Technology
Chembur , Mumbai , India

Bandu B. Meshram
Professor and Head , Computer Department
V.J.T.I, Mumbai

ABSTRACT
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. 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. 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 what the requestor knows i.e. password, challenge response and what the owner has i.e. USB token.

General Terms
Web Application Security

Keywords
Multidimensional password, Novel 3D Ppassword.

1. 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?

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 web sites 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 [2]. This paper presents a new password choice technique. The new technique will be proven secure against shoulder surfing and other form of attacks. This paper is divided

into sections. In section 2, an overview of passwords is presented along with literature survey. The new technique is presented in section 3.

In conducting in-depth online surveys with 324 global IT security decision-makers in November and December 2008, Forrester found that [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.

3. Companies are concerned about the costs of authentication. They want security but without much investment

2. Password and Related Work

Password security is essential to the security of information systems. It is often recommended that passwords not be short, nor words found in the dictionary, and they should be changed frequently. The following rules are used to construct a good password: "A good password – has both upper and lower case letters, has digit and/or punctuation characters as well as letters, is easy to remember, so it doesn't have to be written down, is seven or eight character long, can be typed quickly, so someone else can't look over your shoulder." However, this was in 1991, when brute-force attacks on passwords were not common as they are today. More recent advice is: "When choosing a password, it [sic] really should not contain words found in a dictionary". Because crackers have access to very large on-line dictionaries (with more than 100,000 words), in a number of languages!

- Not be a name of a friend, relative film stars or even a person in a book.
- Not be less than characters in length
- Not be a number.
- Not contain a space

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.

2.1. How the traditional password technique works?

In traditional web application during creation of the account we suppose to enter password and login name with some security questions. This data get saved in database. Next time when user wants to access his account he needs to specify his login name and password. Entered login name and password get compared with one saved in database. If entered login name and password matches with database then only user will get access to his web application. Here purpose of security questions is to retrieve the password when you forget. But problem of this system is anyone can steal the password.

Some system makes use of password salting or hashing to increase the security of password. In cryptography, a salt consists of random bits that are used as one of the inputs to a key derivation function [8]. Figure 1 Shows how it works. The other input is usually a password or passphrase. The output of the key derivation function is stored as the encrypted version of the password. Salt data complicates dictionary attacks that use pre-encryption of dictionary entries: each bit of salt used doubles the amount of storage and computation required. For best security, the salt value is kept secret. To determine a password from a stolen hash, an attacker cannot simply try common passwords (such as English language words or names). Rather, they must calculate the hashes of random characters (at least for the portion of the input they know is the salt), which is much slower. UNIX operating system makes use of salting technique form password storage. In UNIX salt used is time stamp. To avoid storage of passwords, some operating systems store a hash of the password rather than storing the password itself. During authentication system need only verify that the hash of the password entered matches the hash stored in the password database. This make it more difficult for an intruder to get the passwords, since the password itself is not stored and it's very difficult to determine a password that matches given hash.

In next era of password for security many authentication protocols were developed out of them one is challenge response protocol. Challenge response authentication is a family of protocol in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated.

Recently era of password suggest make use of more than one dimension for one time authentication. In paper "A Novel 3D Graphical Password Schema", "Novel Scheme for Securing Passwords" and more have given concept of 3D password[1,2,3,5]. The goal is to design a multi factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment which results in a larger password space. The design of 3D virtual environment, the selection of object inside the environment, and the object type reflect the resulted password space. User has freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more. The 3D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. Advantages of 3D password [5]

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.

In most of the 3D password schema third dimension is thumb impression or photo but the problem with this structure is it requires the extra hardware for capturing photo and thumb impression. Then it will get compare with the one saved in database if there is a match then your login is successful otherwise not.
In available 3D password schema as images are saved in database it consumes more storage space and comparison of images which consumes time. As users need to give thumb impression or photo for authenticating himself, to do that user suppose to make use of hardware like thumb reader or web camp. User should have knowledge of using these devices. One important point is these hardware devices must present on all machines from where user want to access his account. Means it is be dependent on hardware. Some disadvantages of 3D password are listed here
1. More storage space required because it needs to save images which is large binary objects.

2. More cost due to capturing devices.

3. Hardware dependent.

4. Not user friendly user need to know how to use thumb reader or web camera.

In next section we are going to propose a new 3D password schema which will require less space but will provide more security.

3. PROPOSED STRUCTURE

In literature survey we had discussion on 3D password with its advantages and disadvantages. New proposed 3D password has following dimensions first dimension is USB token, second dimension is challenge response and third dimension is login name and password.
How USB tokens works? Tokens are plug into the computer. To use it one must:
1. Connect the token to the computer using an appropriate input device

2. Enter the PIN if necessary.

Depending on the type of the token, the computer OS will now either read the key from token and perform cryptographic operation on it or ask the token's firmware to perform this operation.[7]
Why to use USB tokens? 1. It is secure device, having inbuilt Cryptographic Service Provider (CSP) and Cryptographic processor, used specifically to carry Digital Credentials of individuals and is primarily used for Two Factor authentication. 2. A virus cannot affect USB Token, and the digital Certificate stored would always be secure. 3. USB Tokens offer military grade security and the contents are also encrypted internally. 4 Where as in USB Token, it is simply storing un-signed cheque book in your vault.[6]
Procedure for proposed 3D password will be as follows

1. Specify which web application you want to access.

2. Insert USB token in computer. USB token is first authentication technique in multifactor authentication. Enter the PIN if necessary. Depending on the type of the token, the computer OS will now either read the key from token or it will ask user to enter PIN. Here your pen drive also can act as a USB token if you have configured. But the problem with USB token is anyone can make use of these tokens, that's why we need more dimension for more security. Ones user's USB token is authorized next step it will follow is challenge response protocol

Why this challenge response is required? Some time attacker can steal your USB token and pretend that he is an original user of it. Challenge and response protocol will avoid above problem up to certain extend because response is something which is known to original user only.
Third dimension is user's login name and password for web application. When user supplies proper login name and password he is the authenticated user.
Now the sequence of password is, first specify which application to access then it will ask you to specify login name and insert USB token. Next step is web application server will generate a challenge for client, client supposes to provide appropriate response. If response from user is appropriate then his is the right person. The challenge is a random number and the response is predefined function to challenge. Here challenge generation is only form server side because client needs to be authenticated to the server. Server need not to be authenticated to client. Then user supposes to provide his/ her user name and password.

4. ALGORITHM FOR PROPOSED 3D PASSWORD TECHNIQUE

As we know use of password is divided in two parts one is the password storage and other is storage retrieval.

4.1 Algorithm for password storage

As we know before accessing any web application we need to register with web application following are steps followed.

1. Fill registration form.

2. Negotiate with web application for response function.

5. Register user id and password.

4.2Algorithm for password retrieval

Proposed 3D password consists of following steps. Before using USB token user need to register USB token with web application. User need to specify web application on which he/she wants to work.

1. Specify which application to access
2. Insert the USB token in computer

3. Do USB token authentication.
4. If first step of authorization is successful then generate challenge for user. User will submit response for it.

   If challenge and response is valid means second step of authorization is over display form for login name and password.

   If login name and password matches means third step in authorization is over
   successful login

   Else

   Invalid user

5. Else user is a attacker don't allow access.
6. End

Above algorithm gives you clear working of 3D password

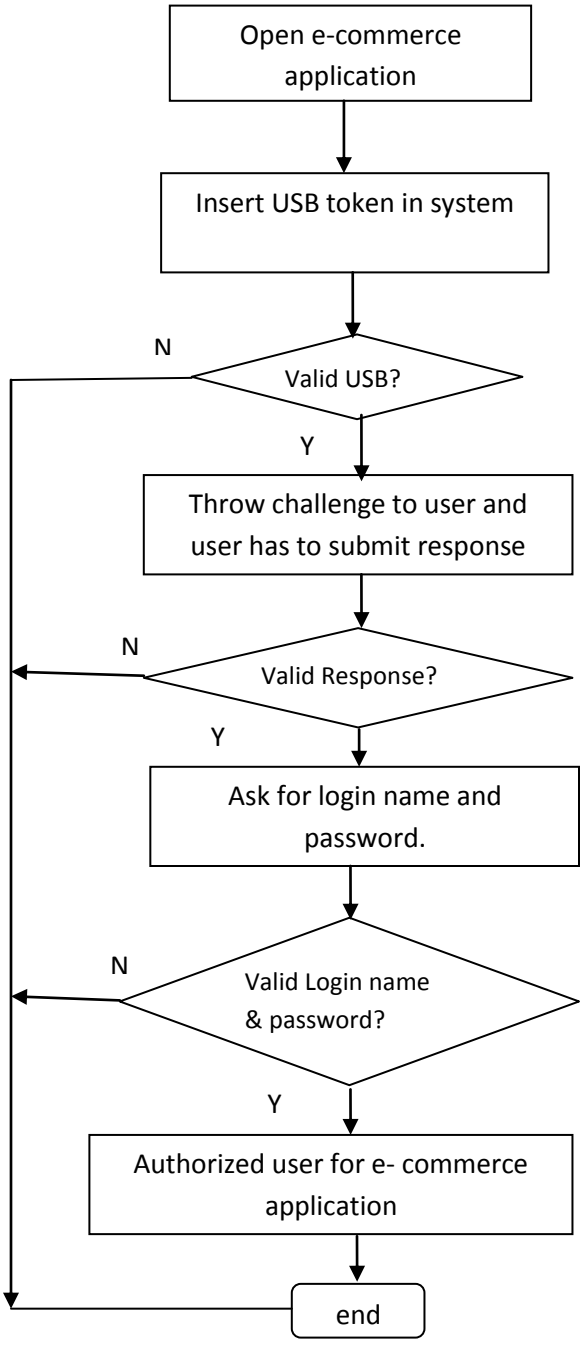

Fig 1 : Workflow diagram of multifactor authentication

4.3 Analysis of proposed 3D password

- This technique is very useful for the application in which user authentication is at highest priority like e-commerce applications.

- As compare to traditional password approach this approach will definitely take more time to do user authentication but it is very secure.
- As compare to other 3D password techniques it require less memory and less cost. As we have discussed your pen drive also can act as USB token no need to invest money for separate hardware. If you want to buy USB token its price ranges from 5$ to 25$ which very less as compare to web camp or thumb reader's price.

  This technique is more users friendly.

5. 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.

Now a day's password security is in high demand. This 3D technique will definitely serve the purpose.

7. REFRENCES

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

[2] Fawaz A Alsulaiman and Abdulmotaleb El Saddik , A Novel 3D Graphical Password Schema Multimedia , VECIMS 2006 – IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems La Coruña - Spain, 10-12 July 2006

[3] Mohammad Shahid, Mohammed A Qadeer, Novel Scheme for Securing Passwords Member, , 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies

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

[5] Three Diamentional password, netlab.cs.iitm.ernet.in/cs648/2009/tpf/cs08m028.pdf

[6] USB Token VS Pen Drive , www.tcs-ca.tcs.co.in/mca21 /html/.../ USBTokenVsPenDrive.pdf

[7] Security tokens, en.wikipedia.org/wiki/Security_token

[8] Forouzan ,"Cryptography and Network Security "

[9]"Authentication-As–A-Service", A commissioned study conducted by Forrester Consulting on behalf of VeriSign, March 20- 2009