Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.552 – 560

Hybrid Approach of 3D PASSWORD Using Naive Bayes Classification

Neha, Mr. Vinod Saroha

Student, Asst. Proff. in CS&IT, Department of Computer Science and Engineering, BPSMV, Khanpur Kalan, Sonepat, Haryana-131001, neha.balhara92@gmail.com, vnd.saroha@gmail.com

ABSTRACT: Users nowadays are provided with major password stereotypes such as textual passwords, graphical password, biometric scanning, tokens or cards (such as an ATM) etc .Mostly textual passwords follow an encryption algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning). Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, etc. which make textual passwords easy to break and vulnerable to dictionary or brute force attacks.

In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.

I. INTRODUCTION:

Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system authentication must be provided, so that only authorized persons can have right to use or handle that system & data related to that system securely. There are many authentication algorithms are available some are effective & secure but having some drawback. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

- Knowledge based: - means what you know. Textual password is the best example of this authentication scheme.
- Token based: - means what you have. This includes Credit cards, ATM cards, etc as an example.

- Biometrics: - means what you are. Includes Thumb impression, etc.
- Recognition Based: - means what you recognize. Includes graphical password, iris recognition, face recognition, etc.

Ideally there are two types of Authentication schemes are available according to nature of scheme & techniques used, those types are

1) Recall based: - In this authentication tech. user need to recall or remember his/her password which is created before. Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

2) Recognition based: - In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used. Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time. To overcome these drawbacks & limitations of previously existing authentication schemes. We have introduced a new authentication scheme which is based on previously existing schemes. This authentication scheme is based on combination of passwords called as "3D Password". Which is a multifactor scheme uses combination of above discussed scheme. All these schemes are implemented in virtual 3D environment while creating 3d Password. Where this environment contain various virtual objects through which user interacts with. The interaction with 3D environment changes as per user changes. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions.

ATTACKS AND COUNTERMEASURES:

To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods. We have to study whether the authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the countermeasures that prevent such attacks. In this section, we try to cover most possible attacks and whether the attack is valid or not. Moreover, we try to propose countermeasures for such attacks.

1) Brute Force Attack: The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

a. Time required to login The total time needed for a legitimate user to login may vary depending on the number of interactions and actions, the size of the 3D virtual environment, and the type of actions and interactions. Therefore, a brute force attack on a 3D password is very difficult and time consuming

b. Cost of attacks the 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all possible biometric information and forge all the required tokens. The cost of forging such information is very high; therefore cracking the 3D password is more challenging. The high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password.

2) Well-Studied Attack: The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well studied attack is very hard to accomplish since the

attacker has to perform a customized attack for every different 3D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

3) Shoulder Surfing Attack: An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical passwords. However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

4) Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign in using the 3D password. This observation gives the attacker an indication of the legitimate user's 3D password length.

However, this kind of attack alone cannot be very successful since it gives the attacker mere hints. Therefore, it would probably be launched as part of a well studied or brute force attack. Timing attacks can be very effective if the 3D virtual environment is poorly designed.

ADVANTAGES

1. Provides security.
2. This 3D password can't take by any other person.
3. 3D graphical password has no limit.
4. Password can change easily.
5. Implementation of the system is easy.
6. Password can remember easily.
7. This password helps to keep lot of personal details.

DISADVANTAGES

1. Difficult for blind people to use this technology.
2. Requires sophisticated computer technology.
3. Expensive.
4. A lot of program coding is required.

II. RELATED WORK:

1. **"3D Login : For More Secure Authentication",**

International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014, ISSN (Print): 2320-9798,

Ashwini A. Khatpe, Dipak V. Waghmare, Ajit S. Shitole,

Student, Assistant Professor, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, India,

Explanation: - 3D password is nothing but a multifactor authentication scheme. Authentication is a necessary element need to provide to any system as it leads to provide more security to that system. But current authentication techniques have some limitations and weaknesses. They are textual

passwords, biometric authentications, graphical passwords, etc. These techniques do not satisfy the security concern regarding authentication scheme completely. A new improved authentication technique is used to overcome the drawbacks of previously existing techniques, which is called as 3D password. In this technique, 3D password is created with help of 3D virtual environment. 3D virtual environment is just a user interface provided to the scheme which looks like same as real environment. 3D virtual environment is consisting of real time object scenarios. User navigates inside the 3D virtual environment and user's interactions towards the objects construct the user's 3D password. This scheme is hard to break and easy to use and also for user, it is easy to remember the 3D password. As 3D password is advanced authentication scheme, it is more secure authentication scheme than any other authentication techniques. In this paper, we present and evaluate our contribution towards 3D Login to the E-mail client system with the help of 3D password to become more secure and more user-friendly to the users. This paper also explains the concept about what is the 3D password, how the Working of 3D password scheme is done, some concepts related to 3D password, applications of the scheme.

2. **"Integration of Sound Signature in 3D Password Authentication System",**

International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 2, April 2013, ISSN (Online): 2320 – 9801,

Mr.Jaywant N. Khedkar, Mrs.Rohini V.Agawane,

Student, Assistant Professor, Dept. of Computer Engineering, KJCOEMR, Pune, India,

Explanation: - Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose their nick names, which make textual passwords easy to break. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards can be stolen. Many biometric authentications have been proposed; however, users tend to prevent using biometrics because of their intrusiveness and the effect on their privacy. Therefore, biometrics cannot be revoked. In this paper, we present the 3-D password. The 3-D password is constructed by sequence of the interactions and actions which performed by users. In other words, the 3D Password scheme is a new authentication scheme that combine RECOGNITION + RECALL+TOKENS+BIOMETRIC in one authentication system. The 3D password can combine authentication schemes such as textual passwords, graphical passwords, and different types of biometrics with supportive sound signature. 3D passwords are flexible and they provide unlimited passwords possibility.

3. **"Implementing 3D Graphical Password Schemes",**

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)

p- ISSN: 2278-8735.Volume 9, Issue 6, Ver. II (Nov - Dec. 2014),

Dr. Mcchester Odoh and Dr. Ihedigbo Chinedum E.,

Department of Computer Science Michael Opara University of Agriculture, Umudike, Abia State,

Explanation: - Beginning around 1999, numerous graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images, parts of images, or sketches. Despite the large

number of options for authentication, text passwords remain the most common choice for several reasons.

4. **"3D Graphical Password Authentication System"**,

International Journal for Research in Applied Science & Engineering

Technology (IJRASET), Volume 3 Issue IV, April 2015, ISSN: 2321-9653,

Mr. Rakesh Prakash Kumawat, Mr. SachinSampat Bhosale,

P.Dr.V.V.Patil Inst.of technology &Engg. (Polytechnic),Loni

Explanation: - Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.

5. **"3D Password: A novel approach for more secure authentication",**

International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5 No. 02 Feb 2014, ISSN: 2229-3345,

Ms. Swati Bilapatte, Prof. Sumit Bhattacharjee,

M. E. (Computer), Department of Computer, MGM College of Engineering and Technology, Email: Email: swatibilapatte.03@gmail.com, sumitnew@hotmail.com

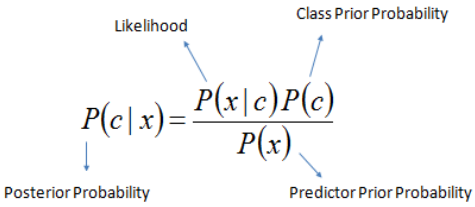
Explanation: - The melodramatic increase of computer usage has given rise to many security concerns. One major security concern is Authentication; process of validating who you are to who you claimed to be. Authentication provides more security to the system. Many existing authentication schemes such as textual password, graphical passwords etc. are available, each one having its own drawbacks and limitations. This paper introduced a new authentication technique, called 3D Password that overcomes the drawback of previously existing authentication schemes. The 3D Password is multi-factor and multi-password authentication techniques that consist of 3D virtual environment containing real time object scenarios. 3D virtual environment is the user interface that looks like same as real time environment but is not actual real time environment. Compared to other authentication techniques 3D Password is more advanced and secure, as it is easy to use and difficult to break. This paper also focuses on explaining what is 3D Password?, how to create 3D password, working of 3D Password and some design principles for designing 3D virtual environment.

III. PROPOSED METHODLOLGY:

3.1 Proposed Method

Proposed authentication scheme is combination of two authentication schemes together. 3D password is combination of both recall-based (i.e. Textual password) & recognition based (i. e. graphical password). So that 3D password is multifactor & multi password authentication scheme. And we are using Naïve Bayes classifier for password authentication in 3D environment which enhance the security.

Naive Bayes (NB): Naive Bayes Classifier uses Bayes Theorem, which finds the probability of an event given the probability of another event that has already occurred. Naive Bayes classifier performs extremely well for problems which are linearly separable and even for problems which are non-linearly separable it performs reasonably well.



$$P(c \mid \mathrm{X}) = P(x_1 \mid c) \times P(x_2 \mid c) \times \cdots \times P(x_n \mid c) \times P(c)$$

Fig1: Naïve Bayes classification

- P(c|x) is the posterior probability of class (target) given predictor (attribute).
- P(c) is the prior probability of class.
- P(x|c) is the likelihood which is the probability of predictor given class.
- P(x) is the prior probability of predictor.

Major advantages of Naïve Bayes Classification is easy to interpret and efficient computation.

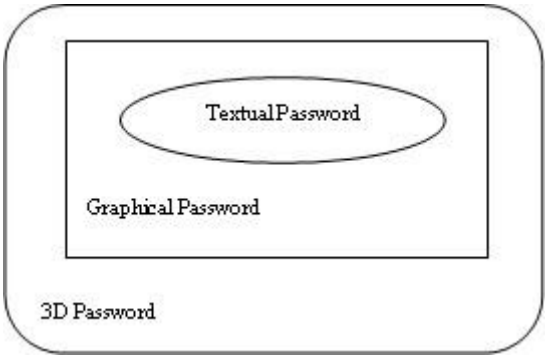


Fig. 1 Multifactor authentication scheme

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate , moving in 3D virtual environment to create a password which is based on both the schemes.

Web servers maintain many files, often hundreds of files. These should be arranged in such a way that users of the application are only meant to see what the website wants them to see. The file hiding concept in this system which can be used by only authenticated users. After successfully authenticated

the user can choose the file on their drive which will be stored on server with user credential which can be later restored by that authenticated user.

IV. Result Analysis / Implementation:

Naïve Bayes Theorem

The naive Bayesian Theorem works as follows:

1. Let T be a training set of samples, each with their class labels. There are k classes, C1,C2, . . . ,Ck. Each sample is represented by an n-dimensional vector, X = {x1, x2, . . . , xn}, depicting n measured values of the n attributes, A1,A2, . . . ,An, respectively.

2. Given a sample X, the classifier will predict that X belongs to the class having the highest a posteriori probability, conditioned on X. That is X is predicted to belong to the class Ci if and only if

$$P(C_i|\mathbf{X}) = \frac{P(\mathbf{X}|C_i)\ P(C_i)}{P(\mathbf{X})}.$$

3. As P(X) is the same for all classes, only P(X|Ci)P(Ci) need be maximized. If the class a priori probabilities, P(Ci), are not known, then it is commonly assumed that the classes are equally likely, that is, P(C1) = P(C2) = . . . = P(Ck), and we would therefore maximize P(X|Ci). Otherwise we maximize P(X|Ci)P(Ci). Note that the class a priori probabilities may be estimated by P(Ci) = freq(Ci, T)/|T|.

4. Given data sets with many attributes, it would be computationally expensive to compute P(X|Ci). In order to reduce computation in evaluating P(X|Ci) P(Ci), the naive assumption of class conditional independence is made. This presumes that the values of the attributes are conditionally independent of one another, given the class label of the sample. Mathematically this means that

$$P(\mathbf{X}|C_i) \approx \prod_{k=1}^{n} P(x_k|C_i).$$

The probabilities P(x1|Ci), P(x2|Ci), . . . , P(xn|Ci) can easily be estimated from the training set. Recall that here xk refers to the value of attribute A_k for sample X.

(a) If A_k is categorical, then P(xk|Ci) is the number of samples of class Ci in T having the value xk for attribute Ak, divided by freq(Ci, T), the number of sample of class Ci in T.

(b) If A_k is continuous-valued, then we typically assume that the values have a Gaussian distribution with a mean μ and standard deviation σ defined by

$$g(x, \mu, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} \exp -\frac{(x-\mu)^2}{2\sigma^2},$$

So that

$$p(x_k|C_i) = g(x_k, \mu_{C_i}, \sigma_{C_i}).$$

We need to compute μCi and σCi , which are the mean and standard deviation of values of attribute Ak for training samples of class Ci.

5. In order to predict the class label of X, P(X|Ci)P(Ci) is evaluated for each class Ci. The classifier predicts that the class label of X is Ci if and only if it is the class that maximizes P(X|Ci)P(Ci).

V. CONCLUSION:

Currently available schemes include textual password and graphical password .But both are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use. The 3-D password is a multifactor & multi password authentication scheme that combines these various authentication schemes. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes. Due to which passwords space increases. The 3D password is still new & in its early stages. The simple and easy design of 3D virtual environment leads to higher user acceptability of the 3D password authentication system. Designing different kinds of 3D virtual environments, deciding on password spaces and understanding user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3D password. Hence this paper tells about our study of 3D password, still it is in early stage. Future work is needed in 3D password scheme to develop this scheme up to more secure level.

REFERENCES

[1] Ashwini A. Khatpe, Dipak V. Waghmare, Ajit S. Shitole, **"3D Login : For More Secure Authentication",** International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014, ISSN (Print): 2320-9798.

[2] Mr.Jaywant N. Khedkar, Mrs.Rohini V.Agawane, **"Integration of Sound Signature in 3D Password Authentication System",** International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 2, April 2013, ISSN (Online): 2320 – 9801.

[3] Dr. Mcchester Odoh and Dr. Ihedigbo Chinedum E., **"Implementing 3D Graphical Password Schemes",** IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), p- ISSN: 2278-8735.Volume 9, Issue 6, Ver. II (Nov - Dec. 2014).

[4] Mr. Rakesh Prakash Kumawat, Mr. SachinSampat Bhosale, **"3D Graphical Password Authentication System"**, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 3 Issue IV, April 2015, ISSN: 2321-9653.

[5] Ms. Swati Bilapatte, Prof. Sumit Bhattacharjee, **"3D Password: A novel approach for more secure authentication",** International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5 No. 02 Feb 2014, ISSN: 2229-3345.

[6] Kalpana Rathi, Nidhi Sharm, Urmila Jangid, **"The survey paper: 3d password"**, International Journal of Innovative Computer Science & Engineering, Volume 1 Issue 3; Page No.06-11, ISSN: 2393-8528.

[7] Mrs. Vidya Mhaske-Dhamdhere, Lecturer., Bhakti Pawar, Pallavi Ghodke, Pratibha Yadav,Student, **"3-D Graphical Password Used For Authentication"**, Int.J.Computer Technology & Applications,Vol 3 (2), 510-519, ISSN:2229-6093.

[8] Tejal Kognule Yugandhara Thumbre Snehal Kognule, **"3D PASSWORD"**, International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012, Proceedings published by International Journal of Computer Applications® (IJCA).

[9] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, **"Secure Authentication with 3D Password"**,International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 2, Issue 2, March 2013, ISSN: 2319-5967.

[10] Nisha Salian, Sayali Godbole, Shalaka Wagh, **"Advanced Authentication Using 3D Passwords in Virtual World"**, International Journal of Engineering and Technical Research (IJETR), Volume-3, Issue-2, February 2015, ISSN: 2321-0869.

[11] Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar, **"New Era of authentication: 3-D Password",** International Journal of Science, Engineering and Technology Research (IJSETR), Volume 1, Issue 5, November 2012, ISSN: 2278 – 7798.

[12] Dhatri Raval Abhilash Shukla, **"Security using 3D Password",** International Journal of Computer Applications (0975 – 8887), Volume 120 – No.7, June 2015.

[13] S. Ranjitha, **"Secure Authentication with 3D Password"**

[14] P.K.Dhanya, M.Keerthiga, S.Dinakar, **"Secured Authentication using 3D Password by Applying Ultimate Planar Algorithm",** International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, ISSN 2229-5518.

[15] Research Scholar,Banita Chadha, Dr. Puneet Goswami, **"3d Password –A Secure Tool",** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014, ISSN: 2277 128X.

[16] A.B.Gadicha, V.B.Gadicha, **"Virtual Realization using 3D Password",** International Journal of Electronics and Computer Science Engineering, ISSN: 2277-1956.

