Volume : 3 | Issue : 1 | January 2014 • ISSN No 2277 - 8179

Research Paper

Two Way Authentication System 3D Password-3 Levels of Security

Engineering

KEYWORDS : Authentication, Textual passwords, 3-D passwords, 3-D virtual environment,Color code

Miss. Nilima D. Nikam Lecturer, Y.T.I.E.T, Karjat

Mr. Amol P. Pande H.O.D COMP, DMCE, Airoli

ABSTRACT

Authentication is any protocol or process that permits one entity to establish the identity of another entity. Authentication is a process of validating who are you to whom you claimed to be or a process of identifying an individual, usually based on a username and password. Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose common words from dictionaries and day to day life, which make textual passwords easy to crack and exposed to dictionary or basic force attacks. Smart cards or tokens can be stolen. Many biometric authentications have been proposed but some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas.

We propose and evaluate our contribution which is a new scheme of authentication. We suggest a hybrid user authentication approach combining text passwords, 3-D passwords, and color code a three-step process, to provide increased security with fewer rounds than such 3-D passwords alone. A variation of this three-step authentication method, which we have implemented and deployed, is new security implementation. This scheme is based on a virtual three-dimensional environment. The 3-D password is a multifactor authentication scheme. Mainly the 3-D passwords are the combination of physical and biometric authentication. The sequence of actions and interfaces 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 conclude the 3-D password key space. 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. 3D passwords are flexible and they provide unlimited passwords possibility. The 3D password's main application is the protection of critical resources and systems.3D passwords have many application areas such as Critical Servers, Nuclear and military Facilities, Airplanes and Jet Fighters, ATMs, Desktop and Laptop Logins, Web Authentication etc. color code provides high level of security. Color codes are difficult to hack. We have also provided security analysis against various attacks such as Brute Force Attack, Well-Studied Attack, Shoulder Surfing Attack, Timing attack etc.

1. INTRODUCTION

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. Current authentication systems suffer from many weaknesses.

Textual passwords are commonly used however; users do not follow their requirements. Graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate user's graphical password by camera. Token based systems such as ATMs are widely applied in banking systems and in laboratories entrances as a mean of authentication. However, Smart cards or tokens are vulnerable to loss or theft. Moreover, the user has to carry the token whenever access required. 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 Biometric scanning.

In this dissertation, we present and evaluate our contribution, i.e., the Two Way Authentication system (3D 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 Authentication system 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. Use of color code makes this system highly secure. Color code provides a solution for shoulder surfing attacks on 3D passwords.

2. AUTHENTICATION

2.1 Authentication

Authentication is any protocol or process that permits one entity to establish the identity of another entity. Different authentication factors: 1.Passwords 2. Tokens 3. Biometrics

2.2 Different authentication systems

2.2.1Centralized Authentication Systems-

Administering local system accounts became impractical as the number of users and systems increased. Developers and administrators moved to a centralized authentication model, which uses a central authority system that can remotely authenticate users across large numbers of systems. Many different systems and protocols were developed for this purpose: remote-authentication protocols such as RADIUS (Remote Access Dial-In User Service), TACACS (Terminal Access Controller Access-Control System), Kerberos, and DIAMETER; and directory-based systems such as Novell's NDS (Novell Directory Services), Microsoft's Windows NT domains, and later, Active Directory.

2.2.2 Multi-Factor Authentication:

Any single factor has its strengths and weaknesses. However, we can increase the reliability and security of the authentication mechanism by combining multiple authentication factors into a single model. For example, ATM cards, as tokens, have their authentication strength increased when they are used by combining them with a PIN number.

The two factors together provide a much higher confidence in the authentication. Tokens are commonly combined with passwords or PINs in a special way to create one-time passwords for use in authenticating to computer systems

2.2.3 Split Authentication:

For the ultra-high-security applications, simply authenticating one user directly against the central authority is not enough, even if all three factors are used. These situations may require authentication to be split among multiple entities, so that the high level of privilege granted by the authentication credential is not abused by a single party. Split authentication is accomplished in the computer world by splitting passwords or cryptographic keys among multiple parties. Many public-key protocols and systems permit, such as PGP, permit splitting keys among

Volume : 3 | Issue : 1 | January 2014 • ISSN No 2277 - 8179

multiple parties, so that messages may be encrypted, decrypted, or signed only when all parties submit their individual part of the split key.

2.2.4 Message Authentication:
It isn't always a user who must be authenticated in the computer world. Sometimes, a message must be authenticated, or at least verified that it has not been altered in transit. This is known as integrity. In this case, a message authentication code (MAC) may be used. A MAC is generated by combining the message with a secret key shared by both the sender and receiver of the message.

3. EXISTING SYSTEM
Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. 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. The password authentication is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. User have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more.

4. PROPOSED SYSTEM
The proposed system is a multifactor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a 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. Proposed system is as follows: We are planning to implement Two Way Authentication system (3D password). In this dissertation there are three stages. In first stage of security user need to provide (Text) 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 3D 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 again receive color code on mobile. User will arrange color code if it is correct, then bank page containing different transaction will be displayed so that different transactions can be performed. System flow is as given below:

Fig.1 System Flow

5. SYTEM IMPLEMENTATION:
5.1 3D Password-The 3D password is a paradigm which is based on a combination of multiple sets of factors. The system of authentication presents a 3D virtual environment to the user where in the user navigates and interacts with the multitude of objects that may be present. The order in which actions and interactions are performed with respect to the objects constitutes the user's 3D password. The 3D password key space is built on the basis of the design of the 3D virtual environment and the nature of the objects selected. The advantage of the 3D password is that it can combine many existing systems of authentication, providing an extremely high degree of security to the user.

3-D password is easily customizable and very interesting way of authentication than before. The concept of 3-D passwords promotes development, diplomacy, and defence as security strategies. It is a multi feature authentication scheme which combines the benefits of different authentication schemes in a single virtual environment. By this user will have the choice to select whether this password will be only recall, biometrics, token or recognition based, or a combination of two or more schemes. User can make infinite number of 3-D passwords by combining any two or more different schemes. Therefore this scheme will be more acceptable to user as it will provide more security than any other authentication schemes. Giving the user the freedom of selection as to what type of authentication schemes will be included in their 3-D password and given the large number of objects and items in the environment(virtual), the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker or say hackers to guess the user's 3-D password. We are using 3D algorithm,MD-5 algorithm for implementing 3D- password .

3D algorithm: The 3D password is a multi factor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

3D PASSWORD SELECTION AND INPUT
Let us consider a 3D virtual environment space of size G ×G × G. The 3D environment space is represented by the coordinates (x, y, z) ∈ [1, . . . , G] ×[1, . . . , G] ×[1, . . . , G]. The objects are distributed in the 3D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3D virtual environment and interact with the objects using any input device such as a mouse, key board, fingerprint scanner, iris scanner, stylus, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3D password. For example, consider a user who navigates through the 3D virtual environment that consists of an office and a meeting room. Let us assume that the user is in the virtual office and the user turns around to the door located in (10, 24, 91) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (4, 34, 18), and the user types "FALCON." Then, the user walks to the meeting room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (1, 18, 30), which is the dot (x, y) coordinate relative to the paper space is (330, 130). The user then presses the login button. The initial representation of user actions in the 3Dvirtual environment can be recorded as follows:(10, 24, 91) Action = Open the office door;(10, 24, 91) Action = Close the office door;(4, 34, 18) Action = Typing, "F"; (4, 34, 18) Action = Typing, "A"; (4, 34, 18) Action = Typing, "L"; (4, 34, 18) Action = Typing, "C"; (4, 34, 18) Action = Typing, "O";(4, 34, 18) Action = Typing, "N".

MD 5 algorithm- MD5 algorithm is used for the authentication purpose. The linked list is stored in a buffer where padding and appending is done to make its length 128 bits. 128-bit sequence is generated by MD5 algorithm. User selects an object in the virtual environment, where password can be stored. As user click on store the password, the 128-bit sequence generated by MD5 is watermarked with the object selected by the user.

5.2 Color code
Color code provides high level of security. Hexaflip cube is used for color code. we have to rotate cube as per color code. Use of color code avoids sholder surfing attack. Color code is use in our system as given below:

The password is "red yellow blue green." Demo 1

Stage 1 cube are by default to orange

Stage 2 flip the cube to get the desired password by default password is set to "red[0],yellow[1],blue[2],green[3]"

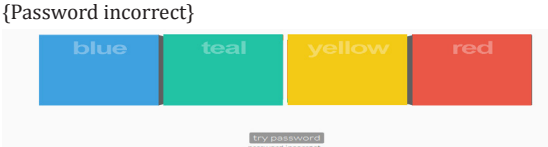
Stage 3 just click on the try password to check the status of the cube

If code is correct it will execute it as {password correct}

Stage 4 if choose another color code then that if will throw an

error

{Password incorrect}



Color code algorithm using permutation combination is used for implementing color code.

6. SCREEN SHOTS:

Fig.2 TEXT LOGIN

Fig. 3. 3D PASSWORD LOGIN

Fig. 4 OTP ON MOBILE

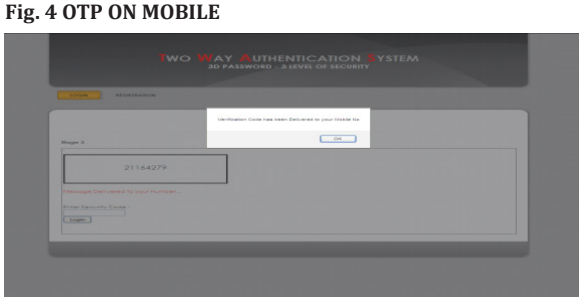
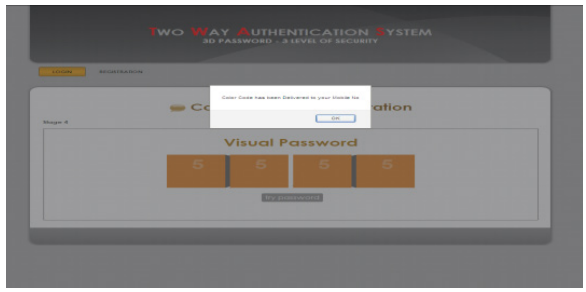


Fig.5 COLOR CODE LOGIN



7. SECURITY ANALYSIS

Attacks and Countermeasures

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
   b. Cost of attacks
2) **Well-Studied Attack** : The attacker tries to find the highest probable distribution of 3D passwords
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.
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.

8. APPLICATIONS:

1.Critical server 2. Nuclear and military facilities 3.Airplanes and jetfighters 4.ATMs 5.Personal digital Assistants 6.Desktop computers and laptop logins 7. Web authentication

9. CONCLUSION

Textual passwords and token-based passwords are the most common used authentication schemes. However, many different schemes have been used in specific fields. Other schemes are under study yet they have never been applied in the real world. The motivation of this work is to have a scheme that has a huge password space while also being a combination of any existing, or upcoming, authentication schemes into one scheme. A 3D password gives the user the choice of modeling his 3D password to contain any authentication scheme that the user prefers. Users do not have to provide their fingerprints if they do not wish to. Users do not have to carry cards if they do not want to. Users have the choice to model their 3D password according to their needs and their preferences. A 3D passwords reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The three-dimensional virtual environment can contain any objects that the administrator feels that the users are familiar with. For example, football players can use a three dimensional virtual environment of a stadium where they can navigate and interact with objects that they are familiar with. The 3D password is in its infancy. A study on a large number of people is required. The main application domains of 3D Password are critical systems and resources. Critical systems such as military facilities, critical servers and highly classified areas can be protected by 3D Password system with large three dimensional virtual environment. Moreover, a small three dimensional virtual environment can be used to protect less critical systems such as handhelds, ATM's and operating system's logins. Acquiring the knowledge of the probable distribution of a user's 3D password might show the practical strength of a 3D password. Color code provides a solution for shoulder surfing attacks on 3D passwords. Combination of Text password, 3D password, color code will provide highly secure authentication system.

REFERENCE

1] 3-D Graphical Password Used For Authentication Mrs. Vidya Mhaske-Dhamdhere, Lecturer.Bhakti Pawar, Pallavi Ghodke,PratibhaYadav,Student,Int.J.Computer Technology & Applications,Vol 3 (2),2008. 2] Graphical Password Authentication Scheme Based On Color Image Gallery Sonkar S.K., Paikrao R.L., Awadesh Kumar, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012. 3]3D PASSWORD - Tejal Kognule ,Yugandhara Thumbre ,snehal kognule(ICACACT)2012. 4] 3d Password: Minimal Utilization Of Space And Vast Security Coupled With Biometrics For Secure Authentication Ms. Nidhi Maria Paul, Ms. Monisha Shanmugham, Volume 2, Issue 4, July 2012 (IJATER). 5] New Era of authentication: 3-D Password,(IJSETR)Volume1,Nov2012.