3-d password for more security

ADVANCED E-SECURITY CP5603 MINOR RESEARCH REPORT Submitted By: Neeraj Kumar MIT-MBA Student ID. : 12682310 TABLE OF CONTENTS Title Page no ABSTRACT 3 INTRODUCTION 2-6 1. 1 Authentication 5 1. Authentication Methods 5-6 1. 3 Organization of the Report 6 ACTUAL RESEARCH WORK 7-8 3D PASSWORD SYSTEM 2. 1 Overview 7 2. 2 Innovative Component 7-8 2. Comparison with Current Authentication Systems 8 IMPLEMENTATION OF THE 3D PASSWORD 9-16 3. 1 Virtual Object Recognition 9 3. 2 3D Password Selection and Inputs 10-13 3. 3 3D VirtualEnvironmentDesign Guidelines 14-16 APPLICATIONS 17-18 4. Advantages 18 CONCLUSION 19 REFERENCES 20 ABSTRACT 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 report mechanism of secure authentication is dicussed. 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. INTRODUCTION In this chapter the 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. Users tend to choose meaningful words from dictionary or their pet names, girlfriends etc. Ten years back Klein performed such tests and he could crack 10-15 passwords per day. On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack.

Which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. 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 strong IR exposure to their retinas (Biometric scanning). In this seminar, 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-Dpassword key space. 1. 1 AUTHENTICATION Authentication is the act of establishing or confirming something as authentic, that is, that claims made by or about the subject are true.

This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what it’s packaging and labeling claims to be, or assuring that a computer program is a trusted one. For example, when you show proper identification credentials to a bank teller, you are asking to be authenticated to act on behalf of the account holder. If your authentication request is approved, you become authorized to access the accounts of that account holder, but no others. 1. 2 AUTHENTICATION METHODS The first is comparing the attributes of the object itself to what is known about objects of that origin.

For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verify the age of an artifact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos. The second type relies on documentation or other external affirmations.

For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost. Currency and other financial instruments commonly use the first type of authentication method.

Bills, coins, and cheques incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify. Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name

goods. 1. ORGANIZATION OF THE REPORT 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-Dpassword key space.

ACTUAL RESEARCH WORK 3D PASSWORD SYSTEM 2. 1 OVERVIEW In this chapter the system consist of multi factor authentication scheme. It can combine all existing authentication schemes into a single 3Dvirtual environment. This 3D virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user’s 3Dpassword.

The 3D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3D virtual environment. The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical password as part of their 3D password. On the other hand users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password.

Moreover user who prefers to keep any kind of biometric data private might not interact with object that requires biometric information. Therefore it is the user's choice and decision to construct the desired and preferred 3D password. 2. 2 INNOVATIVE COMPONENT 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. 2. 3 COMPARISON WITH 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 3D password 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. IMPLEMENTATION 3. 1 VIRTUAL OBJECT RECOGNITION Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions toward the real life objects can be done in the virtual3Denvironment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3Denvironment can be considered as a part of the 3Dpassword.

We can have the following objects: 1) A computer with which the user can type; 2) A fingerprint reader that requires the user’s fingerprint; 3) A biometric recognition device; 4) A paper or a white board that a user can write, sign, or draw on; 5) An automated teller machine (ATM) that requests a token; 6) A light that can be switched on/off; 7) A television or radio where channels can be selected; 8) A staple that can be punched; 9) A car that can be driven; 10) A book that can be moved from one place to another; 11) Any graphical password scheme; 12) Any real life object; 3) Any upcoming authentication scheme. The action toward an object (assume a fingerprint recognition device)that exists in location (x1 , y1 , z1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x2 , y2 , z2), where x1 = x2 , y1 = y2 , and z1 = z2 . Therefore, to perform the legitimate 3Dpassword, the user must follow the same scenario performed by the legitimate user. This means interacting with

the same objects that reside at the exact locations and perform the exact actions in the proper sequence. 3. 2 3D PASSWORD SELECTION AND INPUTS

Let us consider a 3Dvirtual environment space of size G ? G ? G. The 3Denvironment space is represented by the coordinates (x, y, z) ? [1... G]? [1... G]? [1... G]. The objects are distributed in the 3Dvirtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3Dvirtual 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. Consider the sequence of those actions and interactions using the previous input devices as the user's 3Dpassword.

For example, consider a user who navigates through the 3Dvirtualenvironment 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"; • (10, 24,

80) Action = Pick up the pen; • (1, 18, 80) Action = Drawing, point = (330, 130). Figure 3. 2 - Snapshot of an experimental 3-D virtual environment

The 3-D password 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 chieved 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. Fig 3. 2. 1 State diagram of 3D password 3. 3 3D VIRTUAL ENVIRONMENT DESIGN GUIDELINES The design of the 3 D virtual environments affects the usability, effectiveness, acceptability of 3D password. The first step in building a 3Dpassword system is to design a 3-Denvironment that reflects the administration needs and the security requirements. Figure 3. 3 3D virtual environment 1) Real life-similarity

The prospective 3¬D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real life situations. Object responses should be realistic. The target should have a 3D virtual environment that users can interact. 2) Object uniqueness and distinction Every virtual object or item in the 3D virtual environment is different from any other virtual object.

The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3D virtual environment should consider that every object should be distinguishable from other objects. Similarly, in designing a 3-Dvirtual environment, it should be easy for users to navigate through and to distinguish between objects.

The distinguishing factor increases the user's recognition of objects. Therefore, it improves the system usability. 3) Three Dimensional Virtual Environment Size A 3Dvirtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office. A large 3¬D virtual environment will increase the time required by the user to perform a 3Dpassword. Moreover, a large3Dvirtual environment can contain a large number of virtual objects. Therefore, the probable 3-Dpassword space broadens.

However, a small 3D virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time. 4) Number of objects and their types Part of designing a 3D virtual environment is determining the types of objects and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have. For simplicity, we can consider requesting a textual password or a fingerprint as an object response type. Selecting the right object response types and the number of objects affects the probable password space of a 3D password.) System Importance The 3D virtual environment should consider what systems will be protected by a 3D password. The number of objects and the types of objects that have been used in the 3D virtual environment should reflect the importance of the protected system. APPLICATIONS The 3D password can have a password space that is very large compared to other authentication schemes, so the 3D password's main application domains are protecting critical systems and resources. 1. Critical servers

Many large organizations have critical servers that are usually protected by a textual password. A 3-D password authentication proposes a sound replacement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers. 2. Nuclear and military facilities- Such facilities should be protected by the most powerful authentication systems.

The 3D password has a very large probable password space, and since it can contain token, biometrics, recognition, and knowledge based authentications

in a single authentication system, it is a sound choice for high level security locations. 3. Airplanes and jet fighters Because of the possible threat of misusing airplanes and jet fighters for religious, political agendas, usage of such airplanes should be protected by a powerful authentication system. In addition, 3D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system needs.

A small virtual environment can be used in the following systems like Some other application areas: • ATM • Desktop Computers ; laptop logins • Web Authentication 4. 1 ADVANTAGES * Easy to memorize: Users can memorize a 3D password as a " little" story which makes the password easy to remember * Flexibility: 3d passwords allows multi-factor authentication. Smart cards, biometrics and alpha num. password can embedded in the 3d passwordtechnology* Strength: A scenario in a 3D environment offers as almost unlimited combination of possibilities.

As such system can have specific 3d world, hack are extremely difficult. * The 3D password gives users the freedom of selecting what type of authentication techniques. * Secrets those are not easy to write down on paper. * The scheme secrets should be difficult to share with others. * Provide secrets that can be easily revoked or changed. CONCLUSION There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords.

Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various

authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, as mentioned before, both authentication schemes 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.

In this report the 3D password mechanism is explained the 3-D password is a multifactor authentication scheme that combines these various authentication schemes into a single3-D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore, the resulted password space becomes very large compared to any existing authentication schemes. REFERENCES [1] X. Suo, Y. Zhu, and G. S. Owen, “ Graphical passwords: A survey,” in Proc. 1st Annual . Comput. Security Appl. Conf. , Dec. 5–9, 2005, pp. 463–472. [2] D. V. Klein, “ Foiling the cracker: A survey of, and improvement to passwords security, in Proc. USENIX Security Workshop, 2008, Measurement, VOL. 57, September 2008. [3] NBC news, ATM Fraud: Banking on YourMoney, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003. [4] T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). ATMMarketPlace. com. [6] G. E. Blonder, “ Graphical password,” U. S. Patent 5 559 961, Sep. 24, 1996. [7] http://en. wikipedia. org/wiki/3-D_Secure