VEDIO TIME STAMP BASED AUTHENTICATION

P.S. Srinivas

Asst. Professor, Dept of CSE & IT, BVC Engineering college, Palacharla, Rajahmundry.

Abstract: The past decade has witnessed growing interest among researchers to develop graphic password. Authentication as an alternative to text based password authentication. The widely used computer Authentication technique is to supply user name and the password from the standard input devices. These are compared against stored passwords to assure the authenticity of the user. These methods have significant drawbacks. Hardness of the Guessable passwords is directly proportional to hardness of memorizing the passwords. However these Passwords are vulnerable to traditional attack methods like brute force search, dictionary attacks and spyware. Hence to address this problem researchers have developed techniques that use pictures as passwords. Comprehensive analysis done by various researchers suggests that most of the picture based authentication schemes are easily breakable as user tends to click on hotspots in the images. A hotspot is the area of the image which is easily recognized against all other images, thus making such techniques vulnerable. Biometrics based authentication techniques, such as fingerprints, iris scans, or facial recognition has been developed due to unique properties of biometrics. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. This paper suggests a novel solution to address the problems in the existing techniques based on the video time stamps by introducing and implementing a new protocol called "VIDEO TIME BASED AUTHENTICATION PROTOCOL". This protocol uses Video, video time stamps as well as the count of video timestamps and encrypt the time stamp using any cryptographic techniques. This makes it difficult for the intruder to get the time stamps as well as count of time stamps and making this technique more secure, reliable and hard to guess.

Introduction:

There are many widely used authentication methods in the present day scenario which can be broadly classified into three categories. They are as follows

1) Token based authentication

2) Biometric based authentication

3) Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques. A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords. Comprehensive analysis done by various researchers suggests that most of the picture based authentication schemes are easily breakable as user tends to click on hotspots in the images. A hotspot is the area of the image which is easily recognized against all other images, thus making such techniques vulnerable. In this work we suggest and implement a novel knowledge based technique based on the Video time stamps to assure the authenticity of the user. This technique uses Video, Video time stamps and the count of video stamps and encrypt the time stamps using cryptographic methods making it hard for the imposter to guess the password. This method completely eliminates the problem of hotspots that arise in the graphic password authentication.

Existing System

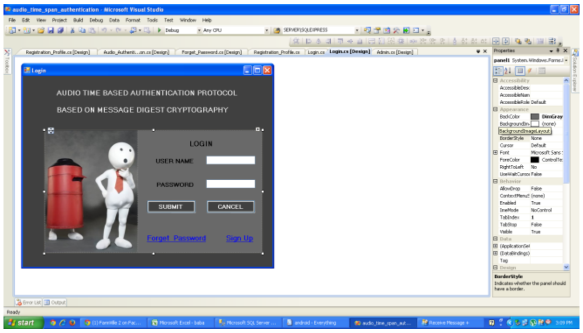
There are two most widely used authentication techniques in the present day scenario.
They are

1) Text Based password authentication

2) Graphic password authentication

Text Based password Authentication

This is the most widely used technique in the present day scenario. In this kind of authentication user enters the password through the keyboard at the time of registration which is stored in the data base. User authentication is done based on the comparison of entered password and stored pass word. Text passwords are the most popular user authentication method but have some security and usability problems. Security problem is nothing but causing various attacks like shoulder surfing (looking over one's shoulder to get information) etc. usability problem refers to limited password space.


audio_time_span_authentication - Microsoft Visual Studio
Login
AUDIO TIME BASED AUTHENTICATION PROTOCOL
BASED ON MESSAGE DIGEST CRYPTOGRAPHY
LOGIN
USER NAME
PASSWORD
SUBMIT
CANCEL
Forget Password
Sign Up
Properties

Graphic password authentication

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption [8]. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices

There are two types of authentication

1. Recall based
2. Recognition based

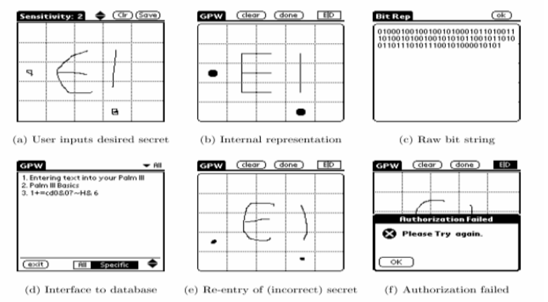
Recall based techniques:

There are two techniques available

1. Reproduce drawing
2. Repeat selection

Reproduce drawing

A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.



01000100100100101000101101001 1
10100101001001010101100101101 0
0110111010111001010000 10101

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

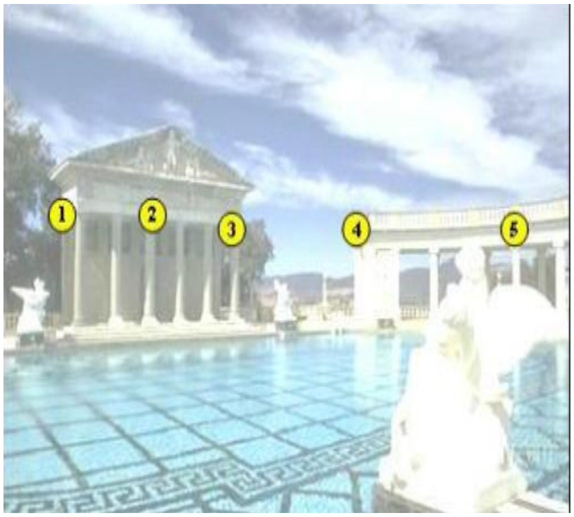
Repeat selection:

To overcome the drawbacks of text based password authentication, graphical passwords had been introduced by Greg Blonder in 1996 which offers another alternative to text password authentication . Graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Passlogix has developed a graphical password system based on this idea. In their implementation (figure 9), users must click on various items in the image in the correct sequence in order to be authenticated The passwords which we are focusing are cued-recall click based graphical passwords (also known as loci metric).In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Examples of these systems include Pass Points (PP) and Cued Click-Points (CCP) which are the present or existing systems.

A. Pass Points (PP):User selects N random points in an image presented to user:

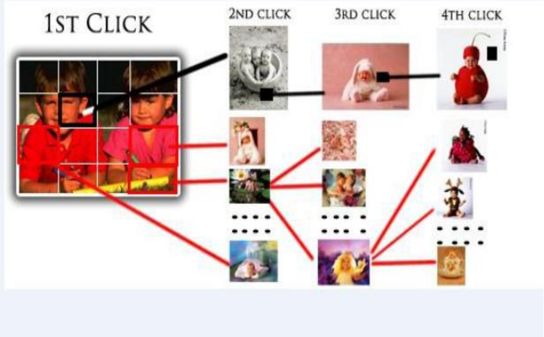
In this system an image is picked from set of images present in a gallery and user is shown the image. Task of user is to click 5 points as shown in Fig 1.As user clicks on the points, features from points are stored and not the point itself. Because storing points directly reduces the security of the technique. As it is very difficult to remember the random points, user chooses to select points on images that can be easily recognized in the image. It is called Hot Spot. Advantage of this system is simplicity of implementation and drawback is low security. In

another variant of this system, user himself picks the image which increases the security. However user has to always enter the same image and within some system-defined tolerance region for each click point during authentication which means that image must be physically present in the client system. Those object(s). For example, if a user decides that people with dark hair are of interest for some reason, the user's attention would shift between objects with features that might indicate a dark-haired person. In the Pass Points graphical password scheme a password consists of a sequence of click points (say 5 to 8) that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point.



Cued Click-Point (CCP):User selects one point in each of N images presented to user randomly:

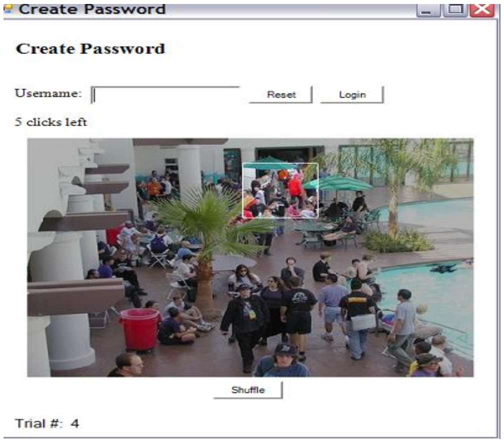
In order to minimize the security loopholes mentioned in pass points system, password distribution scheme is developed. Here user is presented with N random different images and user has to click one point at every image. Based on selected click point of current image next image is displayed randomly by the system as shown in Fig 2.The complexity of this technique is high as user not only has to remember the images in proper order but also has to remember points in every image. This method therefore presents great challenge for the user to remember the password.



Cued Click-Points (CCP).Each click determines the next image. To log in, the user has to click again closely to the chosen points, in the chosen sequence. Since it is almost impossible for human users to click repeatedly on exactly the same point, the system allows for an error tolerance r in the click locations (e.g., a disk with radius r = 10 or 15 pixels).

Persuasive Cued Click Points:

In this technique, an image is displayed to the user and the user is allowed to select 5 click points in the view port of this image. When the user creates a password the all the parts of image are slightly shaded except the view port. A view port is one that highlights a part of the image and the user is allowed to select the click points only in that view port. The view port is positioned randomly rather than specifically to avoid hotspots, since such information allow the attacker to perform the guess work. User must select a click point with in this highlighted view port and cannot click outside the view port unless they press shuffle button to randomly reposition the view port. The view port and shuffle button appear at the time of password creation. At the time of login, images are displayed normally without shading or a viewport and the user may click anywhere on the image.


Create Password

Create Password

Username:

5 clicks left

Trial #: 4

Proposed system

One of the main arguments for graphical passwords is that pictures are easier to remember than text strings.. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords. These graphic passwords suffer from the disadvantages like hotspots. A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of this most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords. Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

Hence to overcome these disadvantages, a novel technique based on video time stamps is developed to assure the authenticity of user. In the profile registration user has to enter his personal details. In the video time stamp registration the user has to select the video and it is played to the user. User is allowed to select n timestamps

Which are encrypted and stored in the database .Security is much strengthened by imposing restrictions on the

failed login attempts. If such restrictions are imposed user is blocked after n login attempts. It is impossible for an imposter to identify the video, number of video timestamps, the sequence of video time stamps.It provides higher levels of security as it is not vulnerable to the password attacks like dictionary attacks, brute force attacks, spyware, guessing and shoulder surfing attacks.

Method:

In this proposed system users selects a video at the time of video time stamp registration which is stored in the database. Video is played to the user and the user is allowed to select a scenario in the video. Whenever user selects scenario, time stamp, at which the selection takes place, is collected. User interface is provided in such a way that the user can select any number of time stamps depending on his interest. Once a time stamp is collected at the time of video time stamp profile registration, it is encrypted using any encryption technique before it is being stored in the data base. At the time of login, User has to repeat the same sequence of timestamps, which he selected at the time of audio time stamp registration, to log on to his/her account .The count of audio time stamps and the exact sequence of time stamps at the time registration and at the login time are compared. If the comparison of timestamps is successful then the user is allowed to log on to account. We can impose restrictions on the number of failed login attempts to provide more security the system. If such restriction is imposed, user is blocked after n number of failed login attempts

The following algorithm is used at the time registration

Algorithm Begin

Step 1: Provide an interface to select the video at the time video time stamp registration.

Step 2: Store the video in the data base.

Step 3 : Get the current time t1

Step 4: Play the video to the user and provide to perform selection

Step 5: When user selects a word/musical note, get current time t2

Step 6: ts = t2-t1 (Ts gives the time stamp at which selection takes place)

Step 7: Apply any Encryption method on ts to encrypt the time stamp and store it in the database.

Step 8: Repeat step1 to step 5 for n times to collect n time stamps

End.

At the time of login the following algorithm is used

Begin

Step 1: Play the same video as selected by the user at the time of registration.

Step 2 : Get the time stamps from the user

Step 3: Compare the count of time stamps at the time of registration and at the login time. If the comparison is successful go to step4 else login fails and display appropriate message to the user. Goto end.

Step 4: If the time stamp sequence at the time of registration and at the time of login matches, user can log on to his account else user fails to login.

Step 5: If user fails to login for 5 successful attempts login fails, user is blocked

End

Security Issues

Here we briefly exam some of the possible techniques for breaking video passwords and try to do a comparison with text-based and graphic passwords.

Brute Force attack:

It is more difficult to carry out a brute force attack against graphical passwords than picture-based passwords. The attack programs need to automatically identify and start the video and generate accurate mouse motion to select timestamp and imitate human input, which is particularly difficult. Overall, we believe a video password is less vulnerable to brute force attacks than a text-based password.

Guessing

Unfortunately, it seems that graphical passwords are often predictable because user tend to pick hotspots. However in the video based authentication the attacker has to identify the video,Video time stamps and a sequence of video time stamps which is very difficult to perform guess work.

Dictionary attacks

Since video time stamp based passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of video passwords. More research is needed in this area to break this passwords. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than graphic and text-based passwords

Spyware

Key logging or key listening spyware cannot be used to break video time stamp basedl passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against time stamp based passwords. However, mouse motion alone is not enough to break video time stamp based passwords

Overall, we believe it is more difficult to break video time stmp based passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against video time stamp based passwords.

Conclusion:

The goal of a good authentication system is to provide the user with a secure password space. Here in the existing system the click point on the image within the scope of the view port area and since the view port cannot be exploited, the password created will be robust. Since shuffling of the viewport increases the time for registration of new users, it is limited. The video time stamp based passwords are more random and strong, so that no hacker can guess it, they are easy to remember as the user select the scenarios in the video. Sometimes scenarios are essay to remember the images. Video based passwords are less vulnerable to traditional attacks. Finally we conclude that video based passwords are more reliable and secure than Text and graphic password authentication techniques

AUTHORS:

1) P.S.SRINIVAS M.TECH is an Asso.Prof in B.V.C.College of Engineering Rajahmundry. His teaching experience spans over two decades to undergraduate and post graduate courses. He developed several software for scientific and commercial applications. He puts up with 20+ years of teaching experience involved in teaching DATA STRUCTURES, DESIGN AND ANALYSYS OF ALGORITHMS, NETWORK SECURITY CRYPTOGRAPHY, DATA MINING, BIG DATA, MOBILE COMPUTING, CLOUD COMPUTING, IOT Etc. His main research is in network Security and Data mining domains.

References:

A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, “SPINS: Security Protocols for Sensor Network”, Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM, 2001.

B. Groza, T.L. Dragomir, "On the use of one-way chain based authentication in secure control systems", Second International Conference on Availability, Reliability and Security (ARES’07), pp. 1214-1221, IEEE Comp. Soc., 2007.

FIPS 180-1, National Institute of Standards and Technology (NIST). “Announcing the Secure Hash Standard”, U.S. Department of Commerce, 1995.

B. Groza, “Using one-way chains to provide message authentication without shared secrets”, Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerU 2006, IEEE Comp. Soc., 2006.

Sonia Caisson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget,Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE “Persuasive Cued Click Points: Design,Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. European Symp.Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007

R. Anderson, F. Bergadano, B. Crispo, J.H. Lee, C. Manifavas, R. Needham, “A New Family of Authentication Protocols”, ACM OSR, 1998.

B. Groza, "Broadcast authentication protocol with time synchronization and quadratic residues chains", Second International Conference on Availability, Reliability and Security (ARES’07), pp. 550-557, IEEE Comp. Soc., 2007.

N. Haller, C. Metz, P. Nesser, M. Straw, “A One-Time Password System”, RFC 2289, Bellcore, Kaman Sciences Corporation, Nesser and Nesser Consulting, 1998.

L. Lamport, “Password Authentication with Insecure Communication”, Communication of the ACM, 24, 770-772, 1981.

F. Bergadano, D. Cavagnino, B. Crispo, “Individual Authentication in Multiparty Communications”. Computer & Security, Elsevier Science, vol. 21 n. 8, 2002, pp.719-735.