AUDIO TIME STAMP BASED AUTHENTICATION

M. Anil Kumar[1] and P.S. Srinivas[2]

1. Asst. Professor (Sr. Grade), Dept of CSE & IT, Sri Sai Aditya Institute of Science & Technology, Surampalem
2. M. Tech Final Year, Dept of CSE & IT, Sri Sai Aditya Institute of Science & Technology, Surampalem

Abstract: An application for assuring the authenticity of audio based information is developed. The application is implemented Media Framework to send audio and video information over RTP (Real-time Transport Protocol). In order to guarantee that information is not altered during transmission over public networks by malicious adversaries some cryptographic functions and protocols are used for achieving information authenticity. More concrete, a cryptographic protocol which uses Message Authentication Codes and elements of a one-way chain as keys is implemented. The solution proves to be efficient and the computational costs are kept to a minimum. A system and methods for permitting open access to data objects and for securing data within the data objects is disclosed. According to one embodiment of the present invention, a method for securing a data object is disclosed. The most common computer authentication method is to use alphanumeric usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods 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. To develop a new authentication protocol based on the audio time stamps making it hard for the imposters to perform guess work. In this work, unique solution is proposed based on audio time stamps by introducing and implementing a new protocol called "AUDIO TIME BASED AUTHENTICATION PROTOCOL". This protocol uses Audio, Audio time stamps as well as the count of audio timestamps and encrypt the password with message digest version 5 and making it hard for the intruder to break the password there by imposing the higher levels of security to the system. The intruder can't get the time stamps as well as count of time stamps and making this technique more secure, reliable and hard to guess.

Introduction:

Sending audio information is a common demand in the present days. Information authenticity refers to a guarantee over the source of information this implies that information was not altered during transmission. However, assuring the authenticity of media information by cryptographic techniques is quite often neglected. Consequently the degree of trust in audio based information sent over public networks is limited since there is no proof that the received information was not altered by malicious adversaries during transmission. In this context assuring the authenticity of audio and video information is a subject of great interest and for this purpose cryptographic techniques are the only alternative, since cryptography is the only security guarantee when we are working with information. This paper is concerned with the development of a application that can be used to capture audio Information and then send it to some remote computers from a public network. More concrete, the application captures images from a web-cam connected to a computer and sends the audio-video information through RTP to other computers. A cryptographic authentication

protocol is implemented in order to prevent information from being altered during transmission. The application of environment provides good support for both managing multimedia streams and implementing cryptography.

The most common computer authentication method is to use alphanumeric usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can easily be guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods 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. In this work, unique solution is proposed based on audio time stamps by introducing and implementing a new protocol called "AUDIO TIME BASED AUTHENTICATION PROTOCOL". This protocol uses Audio, Audio time stamps as well as the count of audio timestamps and encrypt the password with message digest version 5 and making it hard for the intruder to break the password there by imposing the higher levels of security to the system. The intruder can't get the time stamps as well as count of time stamps and making this technique more secure, reliable and hard to guess.

Authentication Process:

- Knowledge based authentication techniques are the most widely used authentication techniques but it is vulnerable to many types of attack such as dictionary attacks, brute-force attacks, spyware, social engineering, shoulder surfing
- Token based authentication 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.
- 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. People tend to forget their passwords due to human memory's fallibility and reminders or replacements are needed. Cost of replacement is anything but negligible and has to be funded. Some users tend to use unsafe practices like writing them down, saving it in email drafts, personal computers, reusing the same password across multiple sites, or frequently reinitializing passwords upon failure to authenticate

Many methods can be used for authentication process but in order to choose the suitable methods for the authentication process, there are a few factors that the researchers preferred. Table 1 shows the comparison of common authentication methods.

Factor	Cost Effective	Secure Level	Drawback
Keycard	Not	Medium	Must carry the token
Password	Yes, but depends on its implementation	Low	Must memorize password
Biometric	Not	High	Must exactly same
Digital Audio	Yes	High	Must exactly same
Prototype System	Yes	High	None

Existing System:

In the existing system we have two different methods for pass word authentication.

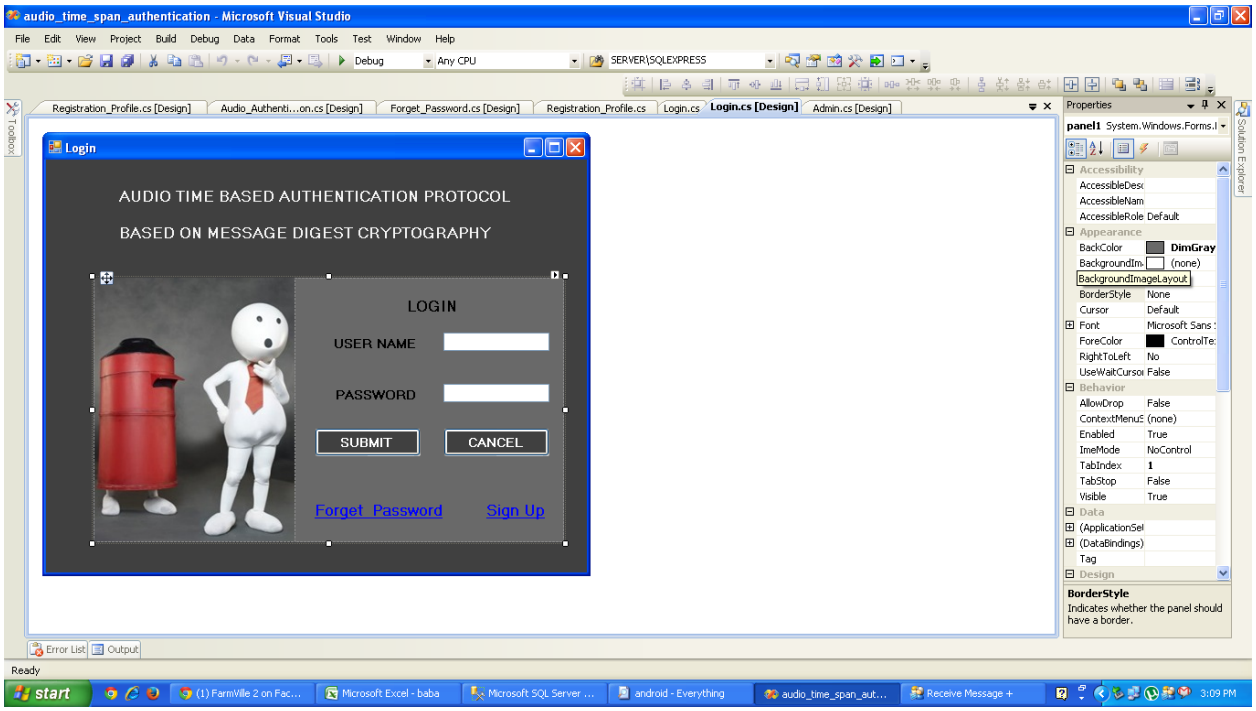
They are

- Text based password authentication

  Text based password authentication process tend to more attendable to attacks such as shoulder hidden camera, Accessing areas. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text based scheme. Because simply adopting graphical

password authentication also has some drawbacks, some hybrid schemes based on graphic and text were developed. In this paper, we proposed a stroke-based textual password authentication scheme. It uses shapes of strokes on the grid as the origin passwords and allows users to login with text passwords via traditional input devices. The method provides strong resistant to hidden-camera and shoulder-surfing. Moreover, the scheme has flexible enhancements to secure the authentication process. The analysis of the security of this approach is also discussed.

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.



Graphic password authentication:

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. 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. 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 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. This authentication technique uses pictures to generate the password. At the time of registration an image/set of images are displayed to the user. User is allowed to select various points on the image/images. At the login time same image/or set of images are displayed to the user and the user is allowed to select various click points on the image or set of images. User authentication is based on the

comparison of sequence of select points at the registration time and at the login time.

Recognition Based Techniques:

A graphical authentication scheme based on the Hash-Visualization technique . In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program . Later, the user will be required to identify the pre selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Background:

Text passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as Password Accentuating systems and tokens have their own drawbacks. Graphical passwords offer another alternative, and are the focus of this paper. Graphical passwords were originally defined by Blonder (1996). In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition based, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage. This project is based on recall based Technique.

Initially when the tolerance limit was large i.e., 5, seven out eight participants entered the correct password and were able to log in. then when the tolerance limit was reduced to a lower value i.e., to 4, only five out of eight participants were able to log in with the correct password. Later when the tolerance limit was reduced to 3 only three of the eight participants were able to log in and when the tolerance limit was reduced to 2 only 2 of the participants was able to log in. finally when the tolerance limit was reduced to 1 no participants were able to log in successfully. So, the experiment shows that the security level increases with the decrease in the tolerance value, which avoid shoulder surfing problem.

lower than the PCCP,s. We suspect that PCCP participants had more difficulty initially learning their password because they were selecting click-points that were less obvious than those chosen by PassPoints and CCP participants. However PCCP participants were ultimately able to remember their passwords with a little additional effort. The experiment shows that security success rate and mean rate of PCCP is very higher than CCP.

Speed and time: In general, CPU speed measure by the amount of work that a given CPU can accomplish in a fixed amount of time. speed and time are inversely propositional, means if it take more time to execute the program then CPU speed is slow and vice versa. Times are reported in seconds for successful password entry on the first attempt. For login and recall, we also report the "entry time": the actual time taken from the first click-point to the fifth click-point. According to user opinion during lab study, The PCCP graphical password authentication system will take more time to executethe program compare to text password and pass point. Because it will take more time to select a click point on 5 different images, but it provides more security

Graphical Password Process:

The purpose of graphical password scheme is to enhance the image-based authentication in both security and usability. There are mainly two steps in this scheme:

- Image selection : In CD-GPS, the first step is the image selection. In this step users have to select several images from an image pool. Suppose there are N1 images in the image pool, then at first users should select n ∈ N1 images from the image pool in an order and remember this order of images like a story. Users should further choose k ∈ n image from the above selected n images. k is nothing but the single image on which we have to draw secret.

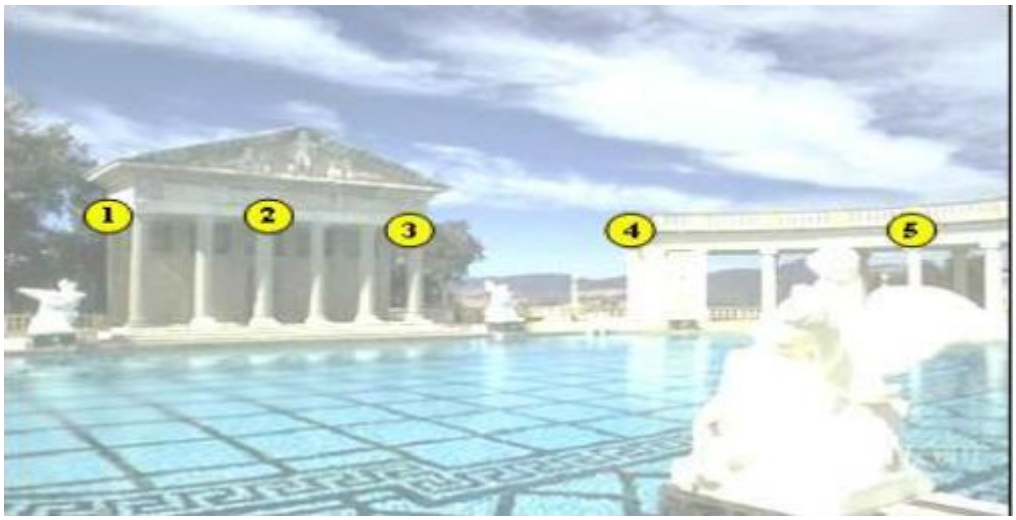
- Secret drawing: This is the second step comes after the image selection. In this step users can freely click-draw their secrets. For constructing secret drawing users use series of clicks

Process Survey:

There are three different techniques available in the graphic password authentication method.
They are
1) Pass points
2) Cued click points
3) Persuasive cued click points.

Pass Points:

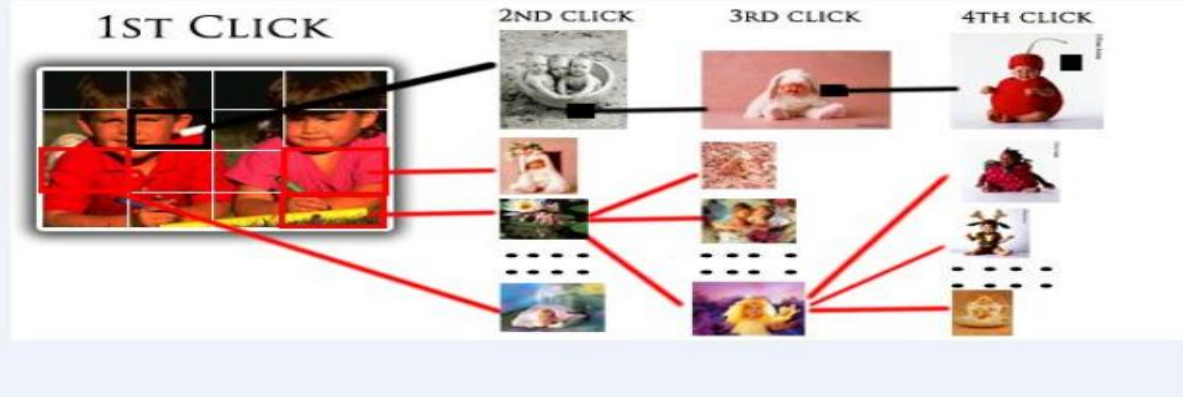
In Pass Points, a password consists of a sequence of five click-points on a given image Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.
It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords.



Cued Click Points:

Cued Click Points (CCP) is another alternative to Pass Points. In CCP, users click one point on each of images rather than on different points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. It also makes attacks based on hotspot analysis more challenging.

As shown in Figure 1, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.



with CCP, users select one click-point per image. The next image displayed is determined by the current click- point.

The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each imagetriggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

User testing and analysis showed no evidence of patterns in CCP, so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem.

Persuasive Cued Click Points:

There are many things that are „well know" about passwords; such as that user can" t remember strong password and that the passwords they can remember are easy to guess [1-6]. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the system" s suggestions for a secure password — a feature absent in most schemes. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click- Points (PCCP) [2], [3], and conducted an in lab-lab usability study with 10 participants. Our results show that our Persuasive Cued Click Points scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. In this paper also analyzed the efficiency of tolerance value and security rate. While we are not arguing that graphical passwords are the best approach to authentication, we find that they offer an excellent environment for exploring strategies for helping users select better passwords since it is easy to compare user choices. Indeed, we also mention how our approach might be adapted to text-based passwords.

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.

.

Proposed system:

In this proposed system an audio is played to the user and the user is allowed to selected words/musical notes in the audio. When ever user selects a particular word/musical note ,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 audio 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 comparision of timestamps is successful,then 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 to get the time stamps.

Begin

Step 1: Get current time t1

Step 2: Play audio and the allow the user to perform selection.

Step 3:When user selects a word/musical note, get current time t2

Step 4: ts = t2-t1 (Ts gives the time stamp at which selection takes place).

Step 5: Apply any Encryption method on ts to encrypt the time stamp and stoe it in the database.

Step 6: 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 audio as selected by the user at the time of registration.

Step2 : 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 comparision is successful goto 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.

User Acceptance Testing

Conclusion: A Dot Net application was developed for sending authentic audio information that is captured from a remote Voicer. The DotNet environment proved to be very useful since both support for managing audio-video content is available in and cryptographic support is present as well. The experimental results show that these protocols are efficient for sending audio information and therefore can be used in practice. As future work we are interested in building a complete solution for

sending authentic audio information which can be efficiently used in many unicast and broadcast scenarios. Our proposed process has various advantages such as it will be hard for attackers to guess the password because using feature of PCCP pattern formation attacks and HOTSPOTS will be removed using viewport & shuffle button. By adding feature of secret drawing to PCCP,attackers fails to know that there is use of secret drawing technique in between these images, unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to be done .The one more advantage is that the message of correct password or incorrect password is displayed after the final click only, by this feature it will hard for attackers to find on which image their guess is correct or incorrect. So by this our proposed scheme will provide higher security in authentication. As an alternative to all these methods, graphical passwords are used because psychology studied that human brain can recognize images better than the text .Graphical passwords are of three types: Click based graphical password scheme, choice based graphical Password scheme and draw based graphical password scheme.Pass-Points: Pass-Point comes under click based graphical password scheme. In Pass-Points password consists of sequence of different click points on a single image. The main disadvantage of this scheme are HOTSPOTS

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.

AUTHORS:

P.S.SRINIVAS M.TECH is a student of final year M.TECH in SRI SAI ADITYA COLLEGE OF TECHNOLOGY,SURAMPALEM,KAKINADA,EAST GODAVARIANDHRA PRADESH.

His main research is in network Security and Data mining domains..

M.ANIL KUMAR M.TECH,(Ph.D)

Is an ASST.PROF IN SRI SAI ADITYA COLLEGE OF TECHNOLOGY,SURAMPALEM,KAKINADA, EAST GODAVARI,ANDHRA PRADESH. He Puts up with 11 years of teaching experience in the field of computer science and involved in teaching DATA STRUCTURES, DESIGN AND ANALYSYS OF ALGORITHMS, NETWORK SECURITY, CRYPTOGRAPHY, IMAGE PROCESSING.

His Main Research is in NETWORK SECURITY AND CRYPTOGRAPHY and he is extensively working in these areas.