IJCAT International Journal of Computing and Technology, Volume 1, Issue 6, July 2014
ISSN: 2348 - 6090
www.IJCAT.org

Session Password Authentication Schemes Using Texts and Colors to Secure Data Backup and Restore for PDA

[1] Narendra Joshi, [2] S.M.Tidake

[1] Computer Engineering Dept., SCOET, Aurangabad, India

[2] HOD of Computer Engineering Dept., SCOET, Aurangabad, India

Abstract - Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder Surfing. These methods are suitable for Personal Digital Assistants.

***Keywords*- DAS, PDA, PIN, AES**

1. Introduction

The most common method used for authentication is text password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the People to store their personal and confidential information like passwords and PIN numbers.

2. Necessity

2.1 Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it's packaging and labeling claims to be.

Methods:-
There are three types of techniques for doing this. The **first type** of authentication is accepting proof of identity given by a credible person who has evidence on the said identity, or on the originator and the object under assessment as the originator's artifact respectively.
The **second type** of authentication 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.

Attribute comparison may be vulnerable to forgery. In general, it relies on the facts that creating a forgery

indistinguishable from a genuine artifact requires expert knowledge, that mistakes are easily made, and that the amount of effort required to do so is considerably greater than the amount of profit that can be gained from the forgery.

In art and antiques, certificates are of great importance for authenticating an object of interest and value. Certificates can, however, also be forged, and the authentication of these poses a problem. For instance, the son of Han van Meager, the well-known art-forger, forged the work of his father and provided a certificate for its provenance as well; see the article Jacques van Meager.

The **third type** of authentication 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.

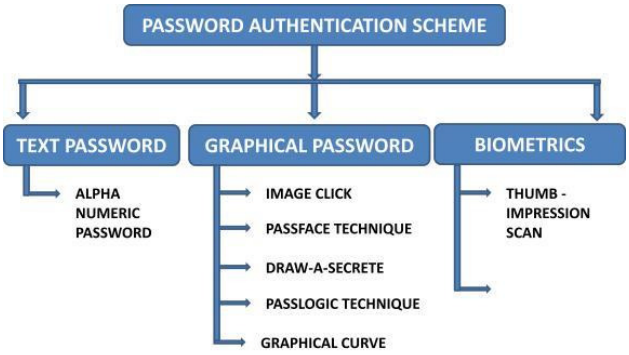
Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods.

2.2. Two-Factor Authentication

When elements representing two factors are required for identification, the term is applied e.g. a bankcard (something the user **has**) and a PIN (something the user **knows**). Business networks may require users to provide a password (knowledge factor) and a pseudorandom number from a security token (ownership factor).

Access to a very-high-security system might require a mantrap screening of height, weight, facial, and fingerprint checks

3. Existing System



Graphical login refers to a class of authentication mechanisms that rely on the creation of graphical images to produce a password value. Graphical login is somewhat similar to visual login and possesses many of the same attributes.

Draw-a-Secret (DAS) is a scheme for graphical password input, targeted for PDA devices [Jer99]. The user draws a design on a display grid, which is used as the password.

The design may include block text as well as graphical symbols. Strokes can start anywhere and go in any direction, but must occur in the same sequence as the one enrolled for the user. Figure 1 illustrates a five-stroke password entry. The numbered items indicate the order in which each stroke was drawn and point to starting end of each stroke. For this five-stroke example, there are 8! different ways it could have been drawn, taking into account both the possible ordering of strokes and, for the three strokes that begin and end in different cells, their possible forward and reverse directions converts it into digital information a computer can A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan.

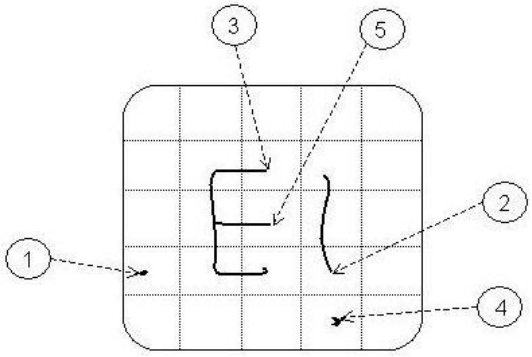


Figure 1. Draw-a-Secret (DAS) technique Proposed by Jermyn

4. Classification of Current Authentication Methods

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication [14]. Currently the authentication methods can be broadly divided into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication [7], also shown in the Figure 1.

4.1 Token Based Authentication

It is based on "Something You Possess". For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site Table 1. [15]. Many token based authentication systems also use knowledge based techniques to enhance security [7].

4.2 Biometric Based Authentication

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits [9]. It is based on "Something You Are" [8].

Dictionary Attack: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.
Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session. In hybrid textual scheme, the randomized hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of s. Even by knowing session password, the complexity is 84.So these are resistant to shoulder surfing.

Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 364. The hybrid textual scheme is dependent on user selection of the s and the ratings. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.If the general order is followed for the s by the user, and then there is a possibility of breaking the system.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368. In the case of the Hybrid Textual Authentication Scheme the complexity depends on s and ratings. The complexity is 8! If ratings are unique, otherwise it is 8.

5. Proposed Solution

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the s in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

5.1. Pair-Based Authentication Scheme

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 7 x 7 and it consists of alphabets, numbers& some special symbols. These are randomly placed on the grid and the interface changes every time.

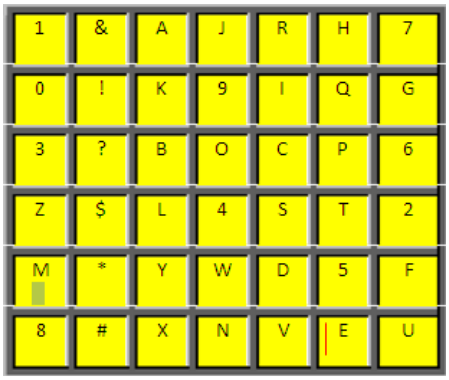


Figure-2 Texts Grid

Figure 3 shows the login interface. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets, digits & some special symbol.

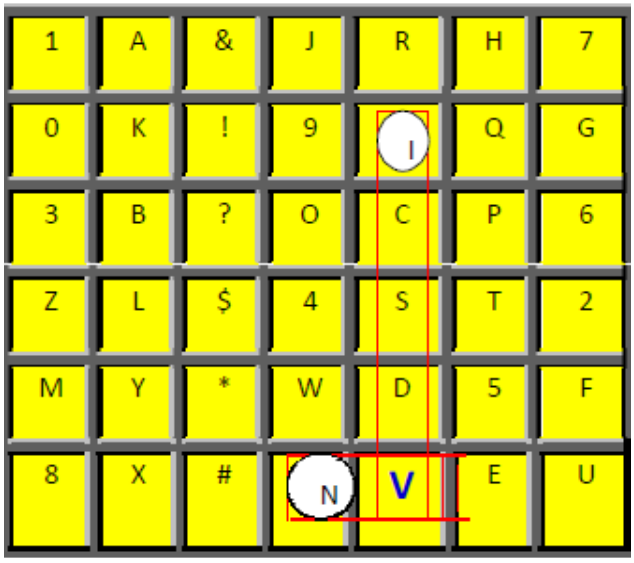


Figure 3: Intersection letter for the pair NI

The first letter is used to select row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 3 shows that V is the intersection symbol for the pair "NI". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password.

5.2 Hybrid Textual Authentication Scheme

During registration, user should rates assign the numbers as shown in figure 4. The User should rates from 1 to 8 and he can remember it as "YRGBOIMP". Same rating can be given to different. During the login phase, when the user enters his username an interface is displayed based on the s selected by the user.

The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of s as shown in figure 4. The grid consists of 4 pairs of colors. Each pairs of represents the row and the column of the grid.

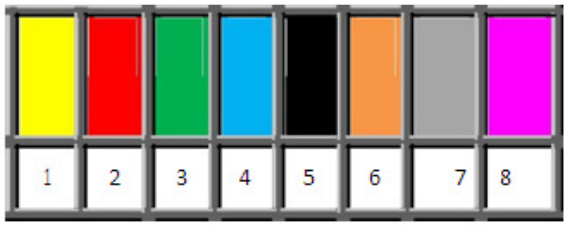
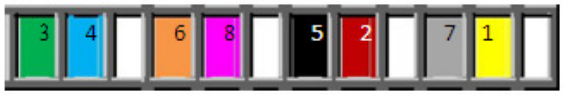


Figure 4: Rating of s by the user



	1	2	3	4	5	6	7	8
1	5	7	8	3	1	4	2	6
2	8	6	4	2	3	1	5	7
3	3	5	6	4	7	8	1	2
4	2	3	5	6	8	7	4	1
5	7	2	1	5	4	6	8	3
6	1	4	7	8	2	3	6	5
7	4	1	2	7	6	5	3	8
8	6	8	3	1	5	2	7	4

LOGIN:

Figure 5: Login interface

Figure 5 shows the login interface having the grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to session password. We get the session password. As discussed above, the first of every pair in grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure 4 ratings and figure 5 login interfaces for demonstration. The first pair has red and yellow colors. The yellow color rating is 1 and red color rating is 2. So the first letter of session password is 3rd row and 4th column intersecting element i.e. **4**. The same method is followed for other pairs of colors. For figure 5 the password is "4524**"**. Instead of digits, alphabets can be used. For every login, both the number grid and the grid get randomizes so the session password changes for every session.

6. Advanced Encryption Standard (AES)

AES is based on the Rijndael cipher developed by

two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES),[7] which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Figure-6 Encryption and Decryption using AES.

6.1 Description of the Cipher

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[8] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

- 10cycles of repetition for 128-bit keys.

□□□□□□□□□□□□□□□□□□□□12 cycles of repetition for 192-bit keys.

□□□□□□□□□□□□□□□□□□□□14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

6.2 AES Algorithm: A Step-By-Step Process

Suppose you are transferring an important message over an unreliable communication channel such as a letter to someone, or simply to give your bank account to someone for transfer purposes. Suppose you are transferring an important message over an unreliable communication channel such as a letter to someone, or simply to give your bank account to someone for transfer purposes.

7. Compliance

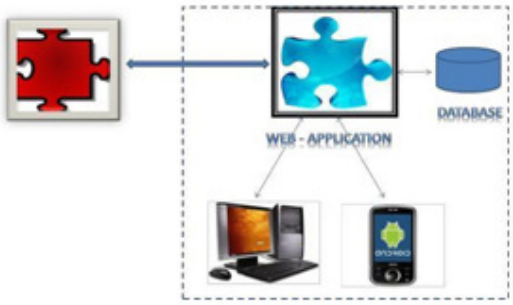


Figure 7 System Model

In the advancing world of technology and the recent explosion of mobile computing devices has resulted in a marked increase in the distribution of information. In our life Smart phones and tablet PCs are making big change.

The most popular operating systems for smart devices are Apple's OS and Google's Android. With the move internet scenario and day-to-day useful applications the amount of data that is exchanged and/or accessed through these smart phones has tremendously increased. Due to limited storage resources and certain security concerns such as lost devices has created the need to backup important data from these smart phones. This thesis work caters to this problem and presents and efficient shared backup and restore model for android device. As hardware resources such as CPU's, memory and batteries are limited in smart

phone. So this work also addresses implementation of the compression module which is basically used while backup and decompressed while restore the data.

8. Conclusion

In this paper, two authentication techniques based on text and colors are proposed for PDAs.These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to s, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

References

[1] R. Dhamija and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.
[2] Real User Corporation: Pass faces. www.passfaces.com
[3] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
[4] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[5] Passlogix, site http://www.passlogix.com.
[6] W.Jansen, "Authenticating Users on Handheld Devices “in Proceedings of Canadian Information Technology Security Symposium, 2003.
[7] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patented. United States, 1996.

Authors Details

Narendra Joshi was born in Nasik, Maharashtra on 1st March 1979.He Received B.Tech Degree (Computer Technology) from Mumbai University in 2004. Presently he is doing M.E. (CSE) last semester student from Shreeyash College of Engineering and Technology, Aurangabad.

Prof. S.M.Tidake work as a HOD of Computer Dept. Shreeyash college of Engineering Aurangabad.