International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013)

Session Passwords Using Grids and Colors for Web Applications and PDA

N. S. Joshi

[1] 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.**

I. 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.

Authentication should be provided for the usage of these devices.

II. Necessity

A. 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 its 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 Meegeren, 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 Meegeren.

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.

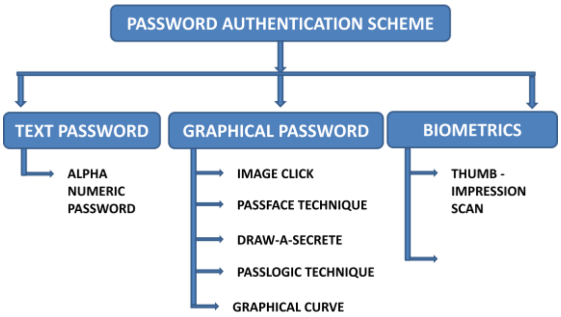
Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheques incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify.

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.

B. 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 (several inherence factor

III. EXISTING SYSTE



A. Graphical Login

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

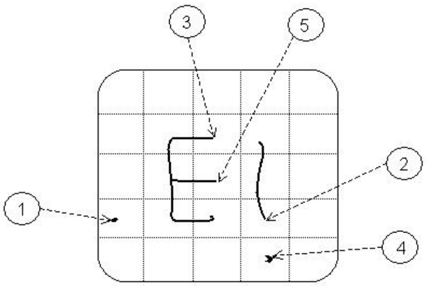


Figure 1. Draw-a-Secret (DAS) technique Proposed by Jermyn

IV. 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.

A. 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].

B. 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 behavioural traits [9]. It is based on “Something You Are” [8]. It uses physiological or behavioural characteristics like fingerprint or facial scans and iris or voice recognition to identify users.

A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify.

Key Features –

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 colors hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of colors. 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 andit is 364 . The hybrid textual scheme is dependent on user selection of the colors 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 colors by the user , 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.

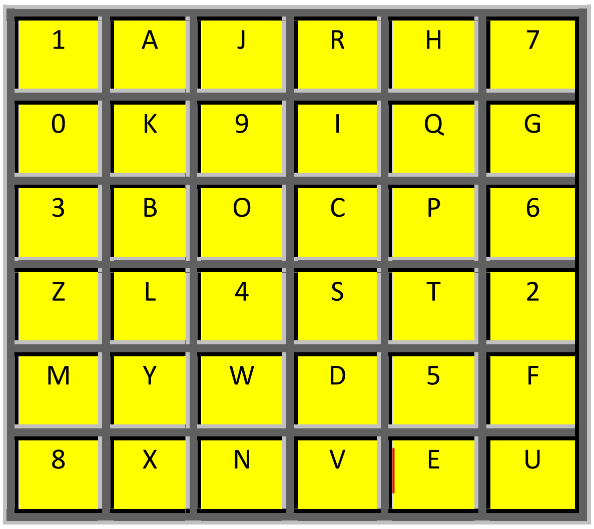
Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368. In the case of the Hybrid Textual Authentication Scheme the complexity depends on colors and ratings. The complexity is 8! if ratings are unique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

V. 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 colors 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.

A. Pair-based Authentication scheme:

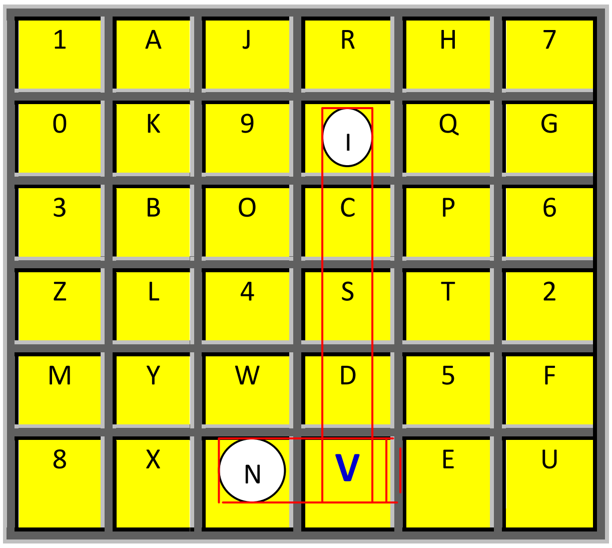
During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.



1	A	J	R	H	7
0	K	9	I	Q	G
3	B	O	C	P	6
Z	L	4	S	T	2
M	Y	W	D	5	F
8	X	N	V	E	U

Figure 2: Login interface

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 and digits



1	A	J	R	H	7
0	K	9	I	Q	G
3	B	O	C	P	6
Z	L	4	S	T	2
M	Y	W	D	5	F
8	X	N	V	E	U

Figure 3: Intersection letter for the pair NI

The first letter in the pair is used to select the 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.

A. Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 4. The User should rate colors from 1 to 8 and he can remember it as "YRGBOIMP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors 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 colors as shown in figure 4. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

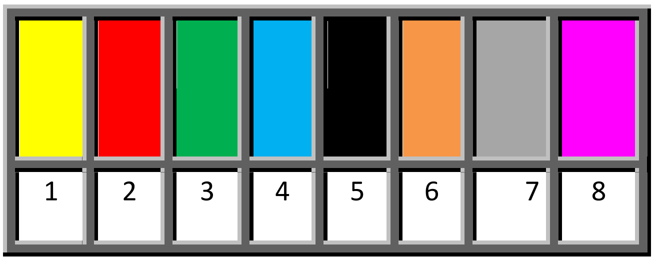
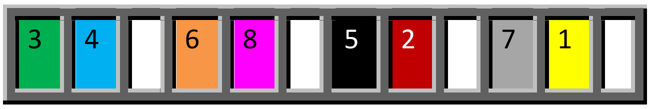


Figure 4: Rating of colors by the user



	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 color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color 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 color grid get randomizes so the session password changes for every session.

VI. Security Architecture Design

Internal Working Steps Taken in Digital Signature with RSA Algorithm:

A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans.

Technology and design methods should be included, as well as the security processes necessary to provide the following services across all technology layers:

1. Authentication
2. Authorization
3. Availability
4. Confidentiality
5. Integrity
6. Accountability
7. Privacy.

In Session Password, we have problem like security of data, files system, backups, network traffic, host security .Here we are are proposing a concept of digital signature with RSA algorithm, to encrypting the data while we are transferring it over the network. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. We proposed digital signature with RSA algorithm scheme to ensure the security of data in cloud. RSA is probably the most recognizable asymmetric algorithm. We include both digital signature scheme and public key cryptography to enhance the security of cloud computing.

In Digital Signature, software will crunch down the data, document into just a few lines by a using "hashing algorithm". These few lines are called message digest. Software then encrypts the message digest with his private key. Then it will produce digital signature .Software will Decrypt the digital signature into message digest with public key of sender's and his/her own private key. We are using Digital signatures so that we are able to distribute software, financial transactions, over the network and in other cases where it is important to detect forgery and tampering.

A Password Security Using RSA-Cryptosystem

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973 by Clifford Cocks of CESG but this was a secret until 1997. The patent taken out by RSA Labs has expired.

The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.

- *RSA Schemes*

RSA Encryption/decryption scheme:

Encryption is done always with public key. In order to encrypt with public key it need to be obtained. Public key must be authentic to avoid man-in-the middle attacks in protocols. Verifying the authenticity of the public key is difficult. When using certificates a trusted third party can be used. If certificates are not in use then some other means of verifying is used (fingerprints, etc).

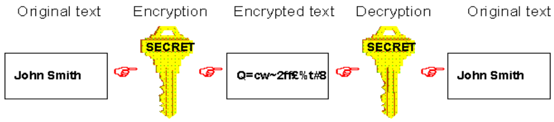
- The message to be encrypted is represented as number *m*, *0 < m < n - 1*. If the message is longer it needs to be spitted into smaller blocks.
- 

Figure 6: Encryption/Decryption method

- Encryption: compute c = m^e mod n, where the e and n are the public key, and m is the message block. The c is the encrypted message.
- Decryption: The private key d is used to decrypt messages.
- Compute: m = c^d mod n, where n is the modulus (from public key) and d is the Private key.

RSA encryption and decryption are not used as much as RSA digital signatures. For encryption usually symmetric algorithms are used instead since they are faster. Sometimes combination of both symmetric key encryption and public key encryption are used to make it faster (PGP).

Things to Remember In Key Generation:

- Key generation is the most important part of RSA; it is also the hardest part of RSA to implement correctly.
- Prime numbers must be primes; otherwise the RSA will not work or is insecure. There exists some rare composite numbers that make the RSA work, but the end result is insecure.
- Find fast implementation of the extended Euclidean algorithm.
- Do not select too small *e*. Do not compute too small *d*.
- Compute at least 1024 bit public key. Smaller keys are now days considered insecure. If you need long time security compute 2048 bit keys or longer. Also, compute always new *n* for each key pair. Do not share *n* with any other key pair (common modulus attack).
- Test the keys by performing RSA encryption and decryption operations.

B RSA 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.

VII. COMPILANCE

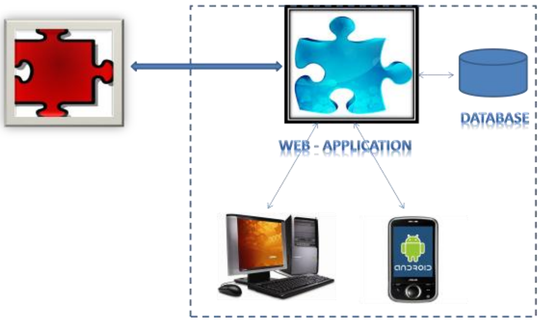


Figure 7: System Architecture

VIII. 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 colors, 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: Passfaces. www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent,Ed. United States, 1996.

[6] Passlogix, site http://www.passlogix.com.

[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.

[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[10] W. Jansen, "Authenticating Users on Handheld Devices “in Proceedings of Canadian Information Technology Security Symposium, 2003.

[11] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[12] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[13] 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.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003