IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Session Passwords using Grids and Colors for Web Applications and PDA

Pragati Patil[1], Nivedita Mhatre[2], Shobhana Gaikwad[3]

Student, Computer Engineering, Bharati Vidyapeeth Institute of Technology, Navi Mumbai, India[1,2]

Professor, Computer Engineering, Bharati Vidyapeeth Institute of Technology, Navi Mumbai, India [3]

Abstract: In authentication, textual password methods are mostly used. But textual passwords are unsafe to eves dropping, dictionary attacks and shoulder surfing, dumpster diving. Graphical passwords are imported as different techniques. Maximum graphical schemes are unsafe to social engineering. To point this problem, text can be combined with images or colors to create session passwords for verification. Passwords can be used once and every time a new password is provoked. There are some procedure which are proposed to developed passwords using colors and text which are resistant to shoulder surfing. Personal Digital Assistance is a relevant technique.

Keywords: DAS, PDA, PIN, Color Code.

I. INTRODUCTION

Relevant method used for authentication is text password. The vulnerabilities of this method like eves dropping, dictionary attack, dumpster diving and shoulder surfing are well known. Rare and long passwords can make the system more protected. But the major problem is the complication of remembering those passwords. The research that results that authorized person selects the smaller passwords or passwords that can be recollected easily[1].
Unfortunately, these passwords can be easily predict or damaged by hackers or the unauthorized persons. Different techniques that are used by the user are graphical passwords and biometrics [2]. Biometrics, such as finger prints, iris scan, speech recognition, hand geometry, facial recognition have been introduced but not yet widely adopted [3]. The major drawback of this avenue is that such systems can be more valuable and the relevant process can be slow. There are some schemes of graphical password that are scheduled last year's [4].But many of them have problem with social engineering techniques which is becoming a huge problem.

II. NECESSITY

A. Authentication
Authentication might require verify the identity of a software program or person, track the elements of arelic, or providing that a product is what its wrapping and labeling requirement to be. There are certain methods:-

The **first type** of verification is taking proof, of identity given by a true person who has proof on the given identity, or discovers and the object under judgment as the originator's relic respectively.

The **second type** of authentication is correlated to the aspect of article itself of that element [5].

For example, an art professional might look for sameness in the style of painting or compares the object to an old photograph. In art and relic, documentation are important for identification of an object of note and assessment. Authentication can, yet, also be false, and the authentication of these acts a problem [6].

The **third type** of authentication expect on documentation or other external confirmation [7]. Example, the rules of confirmation in evidence courts often depend upon beginning the set of custody of confirmation is granted. Currency and other financial instruments are used in the first type of verification method. Bills and cheques consolidate are hard to duplicate physical features, such as printing or inscription, watermarks, and holographic imagery, which are easy for receivers to verify.

Consumer stuff such as perfume, clothing can use either type of authentication manner to avoid forged stuff taking from leading brand's fame. The logo is a lawfully protected or other identifying quality which tends the user in the identification of certain brand-name stuff [7].

B. Two-factor authentication
When elements symbolizing two factors are appropriate for recognition, the term is applied e.g. a card of a bankand a PIN [8]. Business networks may require users to arrange a password and an irregular number from a security demonstration. Approach to a very-high-security system might desire a screening of height, weight, facial, and fingerprint checking, voice/speech reorganization.

III. EXISTING SYSTEM

- Text password
- Graphical password
- biometrics

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

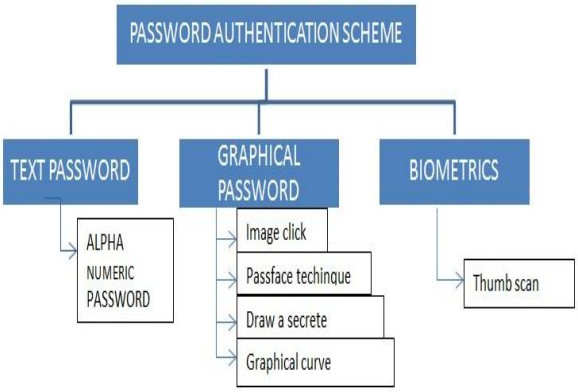

Fig. 1.Traditional Encrypted Search Architecture

A. Graphical Login

Graphical login is assign to a class of certification structure that is built on the formation of graphical pictures to produce a password. Graphical login is somehow identical to visible login and carryout many of the identical aspect.

The design may incorporate block text as well as graphical pattern [9]. Achievement can begin anyplace and go in any order, but must appear in the similar arrangement as the one enrolled for the user. As you can see Fig.1 simplifies a five-stroke password. The specified items pinpoint the sequence in which each stroke was drawn and point to starting end of each stroke. For this 5-stroke part, there are 8! Otherwise it could have been drawn, by taking into an account both of the possible gaining strokes and, for the 3 strokes that begin and end in different cells, their possible forward and reverse directions [10].

V. PROPOSED SOLUTION

There are 3 phases in authentication technique:

i. Registration phase
ii. Login phase and
iii. Verification phase

In first phase, user or person can enters his password in first method and in the second method he can rate the colors. In login phase, the user has to enter the password based on the compound displayed on the screen. The system verifies the password entered by comparing with content of the password develop during registration phase [11].

A. Pair-based Authentication scheme:

During registration the user first submits his password. The length of the password is minimum 8 and it is called as secret pass [12]. Even number of characters is along with in secret pass. Based on this secret pass, term passwords are provoked. In the login phase, when the user enters his username an merge reposing then the grid is shown. The size of grid is 6 x 6.It consists of alphabets or numbers. These are anyway placed on the grid and the interface changes any time [12].

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

Fig. 2 Login interface

Figure 3 shows the login merge. User has to enter the password build upon the private pass. User has to deal with his private pass in terms of pairs. The term password repose 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

Fig 3: Intersection letter for the pair NI

The 1st letters in the combinations are used to select the row and the 2nd letter is used to select the column. The crossing letter is part of the termed password. This is repeated for all combinations of private pass. Fig 3 shows that V is the crossing symbol for the pair "NI". The password enrolled by the user is documented by the server to verify the user. Once the password is correct, the system allowed user to enroll the system. The grid size can be expanded to encompass special characters in the password.

B. Hybrid Textual Authentication Scheme

Inregistration, user should estimate colors as shownin figure 4. The User should estimate colors from 1 to 8 and he can recognize it as "YRGBOIMP" [13]. Same estimation can be given to particular colors. In the login

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

phase, in case user enters his username an interface is shown based on the colors choose by the user. The login interface repose of grid of size 8×8. This grid involves digits 1-8 placed anyway in grid cells. The interface also involves strips of colors as shown in figure 4. The color grid involve of 4 combinations of colors. Every combination of color show the row and the column of the grid [13].

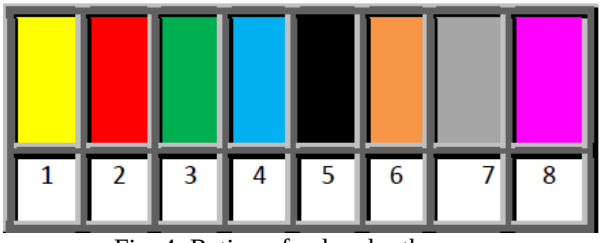

Fig. 4: Rating of colors by the user

	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:

Fig. 5: Login interface

Figure 5 shows the login interface which admits the color grid or number grid of 8 x 8 having numbers 1 to 8 anyway placed in the grid. Lean on the valuation given to colors, we get the termed password. As deliberate above, the 1st color of every combination in color grid shows row and second shows column of the number grid. The number in the crossing of the row or column of the grid is sector of the term password. Suppose the figure 4 estimate and figure 5 login interfaces for presentation. The 1st combination has red or yellow colors. The yellow color valuation of 1 and red color valuation of 2. So the 1st letter of term password is 3rd row and 4th column crossing the element i.e. **4**. The same technique is chased for another combination of colors. In figure 5 the password is "4524**"**. Rather than the digits, alphabets can be used. In every login, couple of the number grid or the color grid get randomizes so the term password switch in whole session.

VI. SECURITY ARCHITECTURE DESIGN

A design and operation of program should also be combined with the explicit system development life cycle to encompass a business case, fundamental definition, design, and operation of plans. Technology and design technique should be encompassing, as well as the secure processes vital to provide the following services beyond all technology layers:

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

In term Password, we admit complication like security of data, files system, backups, network traffic, host security. Here we are recommended a perception of digital signature with RSA algorithm, to encrypting the data during we are dispatching it over the network. A digital signature and digital signature strategy is a mathematical strategy for presenting the legitimacy of a digital memo and certificate. An authentic digital signature gives a reason to accept that the message was generated by a known operator, and that it was not modified in penetration [14]. We recommend digital signature with RSA algorithm strategy establish the security of data in cloud. RSA is apparently the most perceptible asymmetric algorithm [2]. We encompass the couple of digital signature strategy and public key cryptography to build up the security of cloud computing [7].

For Digital Signature, software will crisis down the data, archived into just a minor lines by a using "hashing algorithm". These minor lines are labeled as message digest. Secret key is encrypted by his message digest in software [16].

Then it will yield digital signature .Software will Decrypt the digital signature into message digest with public key of operator and his/her own secret key.

We are using Digital signatures so that we are able to assign the software, financial transactions, over the network. Otherwise, where it is essential to catch forgery and tampering [17].

VIII. CONCLUSION

In this paper, two authentication procedures depend on text or colors are recommended for PDAs. These techniques create term passwords and are defiant to dictionary attack, brute force attack and shoulder-surfing. The couple of these techniques uses grid for term passwords propagation. Combination based technique desires no special type of certification, in the course of login time depend on the grid displayed a term password is achieved. In hybrid textual strategy, valuation should be given to colors, depend on these valuation and the grid advertised during login, term passwords are provoked. Yet

these strategies are completely new to the users and the recommended authentication techniques should be documented broadly for usability and effectiveness.

ACKNOWLEDGEMENT

Thanks to our guide, and our college management for providing the resources and helping us in all the possible ways. We also thank readers of this journal for reading this topic and contributing towards the enhancement of this topic as well.

REFERENCES

[1] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.
[2] Authentication Schemes for Session Passwords using Color and Images www.scribd.com/document/73912795
[3] www.asmgroup.edu.in/incon/Incon-%
[4] ALSULAIMAN, F. A. & EL SADDIK, A., 2008, „Three-Dimensional Password for More Secure Authentication", IEEE Transactions on Instrumentation and Measurement, vol.57, pp.1929-1938
[5] TechNet. (2012). Dynamic Access Control: Scenario Overview. Retrieved August 2, 2012, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/hh831717.aspx
[6] A letter to the Royal Society presenting A new theory of light and colors Isaac Newton, 1671
[7] Committee on National Security Systems. "National Information Assurance (IA) Glossary" (PDF). National Counterintelligence and Security Center. Retrieved 9 August 2016.
[8] BIOIDENTIFICATION www.bromba.com/faq/biofaqe.htm
[9] Cognition and Instruction/Print version.
[10] www.biostars.org/p/3423/
[11] M Sreelatha, M Sultan Ahamer, M Shashi , V Manoj Kumar , M Anirudh 1, "Authenticationv Schemes for Session Passwords using Color and Images".
[12] F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Writtenwith Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[13] Berners-Lee, T., Hendler, J., &Lassila, O. (2001, May). The Semantic Web. Retrieved April 10, 2007, from Scientific American.com:http://www.sciam.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21
[14] Internet Security Policy: A Technical Guide by Barbara Guttman and Robert Bagwill: National Institute of Standards and Technology Computer Security Division http://csrc.nist.gov/
[15] research.ijcaonline.org/etcsit/nuwww.pgpi.org/doc/pgpintro/article. sciencepublishinggroup.co
[16] www.c-sharpcorner.com/UploadFile/
[17] sameekhan.org/pub/Q_K_2013_IP.