One Time Password Generation for Multifactor Authentication using Graphical Password

Nilesh B. Khankari[1], Prof. G.V. Kale[2]

[1,2]Department of Computer Engineering, Pune Institute of Computer Technology,

Pune, India

[1]nilesh111khankari@gmail.com, [2]gilkale@gmail.com

Abstract— Single factor authentication such as password authentication is no longer considered as secure in the Internet world. There is a rapid growth in demand for strong authentication on the highly critical web-based applications. A higher level security mechanism is needed to access the financial and banking applications. Existing system provides authentication mechanism based on the static password, personal identification number (PIN) etc. These methods are vulnerable against eavesdropping and replay attack. In this work, a two factor authentication scheme is proposed for user authentication. The presented scheme generates dynamic password for two factor authentication. This scheme will provide user assurance of authentication and will improve authentication level. The proposed scheme provides strong protection against cryptanalysis.

Keywords— Security and protection, Authentication, Graphical Password.

INTRODUCTION

Authentication is process in which right user will be given access to resource. During authentication only authorize user will get access to resources. There are various types of methods available for authentication. Multifactor authentication uses the combination of more than one technique for authentication. More than one form of authentication used in multifactor authentication that's why multifactor authentication. Multifactor authentication provides extra layer of authentication which minimizes risk in risk based authentication.

In today's world to access critical resources authentication is required. To secure our critical resources more secure authentication is necessary. Authentication is process in which authorized user (i.e user which has rights to access particular resource) will be given access to resource. During authentication only authorize user will get access to resources. For example user who needs to perform internet banking operations is required to provide authentication details to access his internet banking account.

In this paper, we analyzed current existing authentication schemes, proposed an effective dynamic user authentication scheme. The proposed system generates dynamic password using seed factors which are associated to graphical password and random string. Thus using this proposed scheme identity and access manager system will be secured from Brute-force attack, especially Perfect-Man-In-The-Middle attack.

RELATED WORK

There are various types of techniques established for authentication. Most widely used and traditional authentication technique is alphanumeric password. This password consists of secret series of characters. The user id and password act as user identification and authentication to access required resources. This technique secures resources but it has many disadvantages .In this technique user picks password which is easily guessed and vulnerable to shoulder surfing. When user selects difficult to guess text password then it is hard for user to remember password and thus compel the users to write them down, which impairs their secrecy. Also dictionary attack, brute force attack, spyware is possible in this method. Password can also be system generated but these passwords are difficult to remember.

To overcome the problems related to traditional text password method some researchers developed authentication methods that uses pictures as password. [2], proposed recognition based a graphical password mechanism. In this user is asked to select certain no of images from given set of images as a password. Later, for authentication user has to select previously selected images. Graphical passwords are more difficult to break using the traditional attack methods such as brute force search, dictionary attack, or spyware.

Another way for authentication is biometric based authentication. Biometric based authentication uses certain physiological or behavioral characteristics which are unique for each person [3].

Luigi Catuogno and Clemente Galdi proposed a PIN-based mechanism is presented that uses a secret sequence of objects to analyze security vs. usability. This work does not consider the use of contextual information to influence the generation of the challenge [4]. Jakobsson M., et.al introduced the notion of implicit authentication that consists in authenticating users based on behavioral patterns [5]. Xuguang Ren, Xin-Wen Wu proposed generation of dynamic OTP. They have considered user's password, the authenticating time, as well as a unique property that the user possesses at the moment of authentication (for example, the MAC address of the machine that the user uses for authentication) to generate OTP. This system effectively protects user's account against various attacks such as phishing attack, reply attack, and perfect-man-in-the-middle attack [6]. Hayashi E., et.al present a framework is presented that combines passive factors (e.g. location) and active factors (e.g. tokens) in a probabilistic model for selecting an authentication scheme that satisfies security requirements; however, it does not consider client device constraints [7]. Huiyi L. and Yuegong Z proposed scheme which uses two one-way hash functions, one is a hash chain-which is the core of the authentication scheme, and the other is used to secure the hash chain for information transmission between the user and server. This scheme provides functions of bidirectional identity authentication and presents higher security and lower computational cost [8]. Yair H., et.al proposed context-aware multi-factor authentication scheme based on a Dynamic PIN. The scheme presented in this paper produces a graphical challenge for this authors considered context, client device constraints, and risk associated [9]. Jeonil Kang, et.al in this paper, a two-factor face authentication scheme using matrix transformations and a user password is suggested [10]. Soon-Nyean Cheong, et.al presented a secure two-factor authentication NFC smartphone access control system using digital key and the proposed Encrypted Steganography Graphical Password [11].

Mathematical Model

Let S be a system such that S ={s, e, X, Y, C, R, f, $f_{friend,}$| Φ}
Where, s is the start state.
e is end state.
X is Input of the system.
Y is output of the system.
f is set of functions in the system.
$f_{friend,}$ is set of friend function used in system.
Φ is constrains to the system.

C= (I_1, $I_2 \ldots I_n$) be a set of n image objects.
Where I_i is image object which can be icon, animal picture etc.

R = (r_1, $r_2 \ldots r_n$) be the vector of seeds.
Where r_i is seed factor related to each image object $I_{i.}$

X = {Pass}
Pass is the password entered by user. Pass⊂ C

Y = {DynPass}
DynPass is dynamic password generated by system.

f_{friend} = {S(X), Rand}

S is Rijndael substitution box function which takes 2byte number(X) as input and generates 1byte number.

Rand is function used to generate random number or string.

f = {Challenge(C), V (Pass), G (UserPassword, RS)}

Challenge function will generate image challenge for user for authentication. Input for this function is C i.e. set of image objects. Output of this function will be ChallengeImages.

ChallengeImages=Union(SecretImages,NonSecretImages) with cardinality |q+p|

|SecretImages|=q, |NonSecretImages|=p

V is validation function which validates user.
SecretImages is set of images selected as a password when user registered as a new user.
If Pass = SecretImages then user is validated. If user is authorized user then it generates UserPassword.
UserPassword is 2 bytes long number, that is, each hexadecimal digit hex_i is a nibble (half byte).

$$\text{UserPassword}=\text{XOR }(r_{1'},r_{2'},r_{3'}\ldots..r_{|\text{secretImages}|}) = hex_1 hex_2 hex_3 hex_4$$

G is dynamic password generation function. This function takes UserPassword and RS as input.
RS is random generated 8 byte string.
$RS = RB_0RB_1RB_{2\ldots}RB_7$ where RB_i is a byte.
So output of function G is DynPass.
DynPass = $byte_1byte_2byte_3byte_{4.}$

This password is generated using S-Box function S(X). Each $byte_i$ digit is computed from 4 substitutions between UserPassword (2 bytes long) and 2 bytes of RS and 4 iterations through the s-box S(X) then after XOR operation will be performed on results of 4 iterations. Fig. 1 shows the sequence of iterations and substitutions to produce $byte_1$. In the diagram each arrow indicates one iteration through S(X). During each iteration, S(X) takes as input one byte consisting of two nibbles: a hexadecimal digit of UserPassword and a nibble of RB_i; and outputs a new byte, hereafter S_i. The following are the 4 iterations performed to generate $byte_{1.}$

$$S(hex_{1,}RB^{H}{}_{0})=S_1$$
$$S(hex_{2,}RB^{L}{}_{0})=S_2$$
$$S(hex_{3,}\ RB^{H}{}_{1})=S_3$$
$$S(hex_{4,}\ RB^{L}{}_{1})=S_4$$

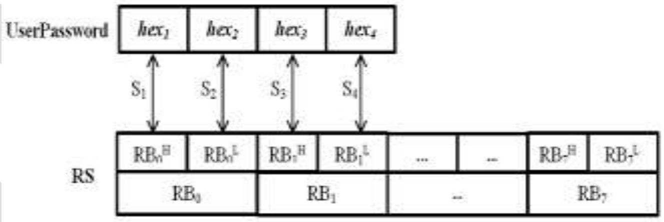

Fig.1 Chain of iterations to generate $byte_1$

$$(S_1 \text{ XOR } S_1 \text{ XOR } S_1 \text{ XOR } S_1) = byte_1$$

PROPOSED SYSTEM

As per survey, current existing systems have problems and don't give more randomness. So I have proposed a new multifactor authentication method which has more randomness.

Proposed system has 2 phases: 1. Registration and 2. Login.

1. Registration :

1.1 Registering the Image-Based Password(s). The user is presented with image objects C. A randomly generated number is linked with each image object I_i. Let R = (r_1, r_2…r_n) be the vector of seeds. Length of each r_i is 2 bytes and represented as 4 hexadecimal digits. User has to select number of images as a password from given images.

2. Image Challenge and Dynamic Password Generation:

Steps:

i. The server generates a random string (RS) and the graphical challenge. The RS is used as part of the dynamic password generation algorithm. The challenge is constructed by combining secret and non-secret images.
ii. The user is asked to recognize the secret images.
iii. The crypto-function is then used to generate the dynamic password.
iv. The client device sends the dynamic password to the server for validation.

2.1 Generation of RS and Image Challenge:

- Random Strings: RS is pseudo-randomly generated string of 8 bytes.
  $RS = RB_0RB_1RB_{2\ldots}RB_7$ where RB_i is a byte.

- Image Challenge:
  This step will generate image challenge for user for authorization. Challenge function will generate image challenge.

2.2 User Response to Challenge:

- User responds to the challenge by selecting secret images.
- Algorithm selects random number linked with secret images and performs XOR operation on them to generate UserPassword.

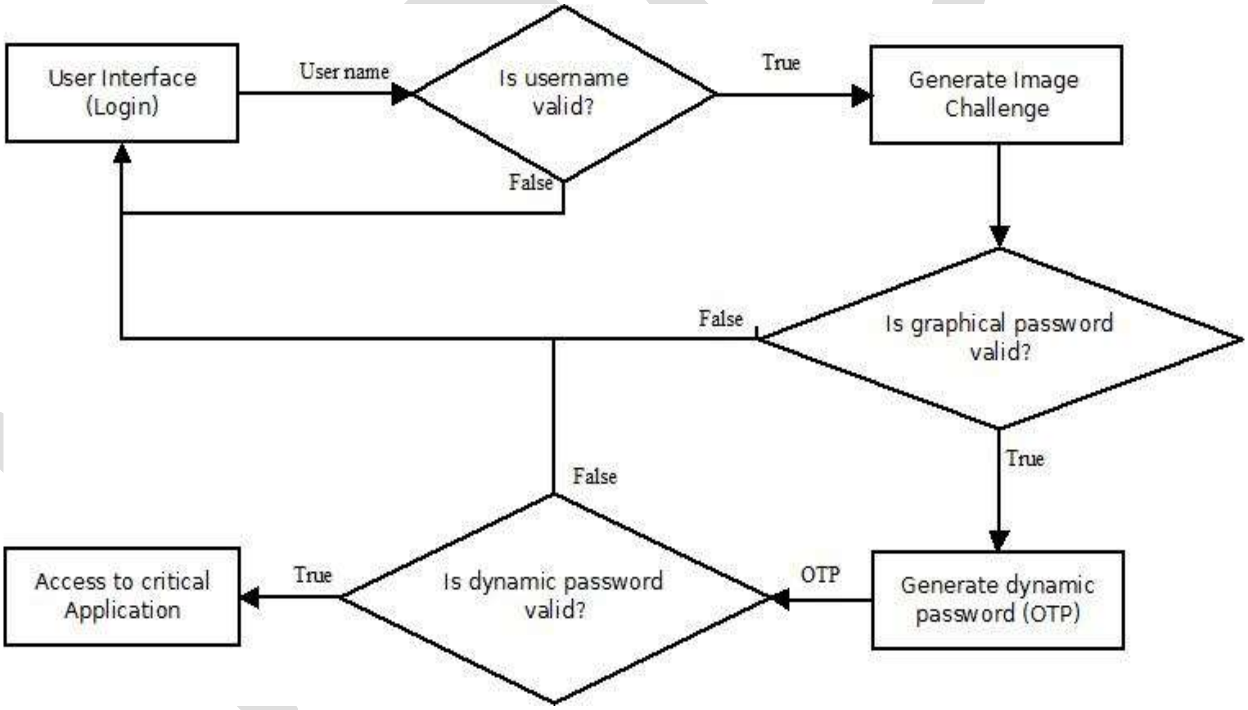
User Interface (Login)
User name
Is username valid?
True
Generate Image Challenge
False
Is graphical password valid?
False
True
False
Access to critical Application
True
Is dynamic password valid?
OTP
Generate dynamic password (OTP)

Fig.2 System flow

2.3 Generation of Dynamic Password:

A Substitution Box (S-Box) is a component used in cryptosystems to perform substitutions in a way that relations between output and input bits are highly non-linear. This protects against cryptanalysis. An S-Box designed to be resistant to linear and differential cryptanalysis is the Rijndael S-Box. Function G will generate dynamic password.

RESULTS AND ANALYSIS

Fig.3 shows image challenge generated for user authorization In proposed system images are recognized in random order (not sequentially). Numbers of possible combinations are $! / (n - q)!\, q!$.

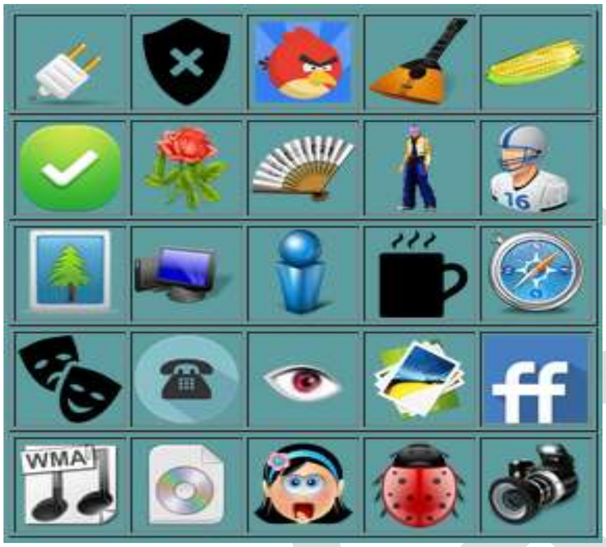

Fig.3 Image challenge

In proposed system user has to recognize 5 icons from 25 provided icons. So p=5, q=20 and n=25 i.e. 53130 combinations are possible. UserPassword is generated after valid graphical password is entered. UserPassword is number generated by performing XOR operation 5 random numbers which are linked with 5 secret images. Suppose this 5 random numbers are 21546, 31289, 12678, 30876, 20369 on this 5 numbers XOR operation will be performed and this will generate number 10100010011000 which is in binary format. As mention in mathematical model generated number after performing XOR operation on 5 random numbers and RS are inputs to function G. Function G will generate dynamic password.

CONCLUSION

Here, we have analyzed the disadvantages of existing authentication schemes, proposed an effective dynamic user authentication scheme. The proposed system integrates the security techniques Image Based Password Authentication and one time password based on Image Based Password. The proposed system generates dynamic password (OTP) using seed factors which are associated to graphical password and random string. Thus using this proposed scheme critical application will be secured from Replay attack, Dictionary attack, Brute-force attack, especially Perfect-Man-In-The-Middle attack. Using proposed dynamic password generation scheme there is improvement in user assurance of authentication.

REFERENCES:

[1] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," Computer Security Applications Conference, 21st Annual. IEEE, pp. 10-19, 2005.

[2] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," Proceedings of 9th USENIX Security Symposium, 2000.

[3] Wayman, J., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2004). Biometric systems: Technology, design and performance evaluation. New York: Springer.

[4] Luigi Catuogno, Clemente Galdi,"A Graphical PIN Authentication Mechanism with Applications to Smart Cards and Low-Cost Devices", Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, LNCS, vol. 5019, pp. 16–35, 2008.

[5] Jakobsson M., Shi E., Golle P., Chow R.," Implicit authentication for mobile devices", Proceedings of the 4th USENIX Conference on Hot Topics in Security, p. 9. USENIX Association, 2009.

[6] Xuguang Ren, Xin-Wen Wu, "A Novel Dynamic User Authentication Scheme", International Symposium on Communications and Information Technologies, pp. 713-717, 2012.

[7] Hayashi E., Das S., Amini S., Hong J., Oakley, "CASA: context-aware scalable au-thentication", Proceedings of the Ninth Symposium on Usable Privacy and Security, pp. 1–10. ACM, Newcastle 2013.

[8] Huiyi L., Yuegong Z., "An Improved One-time Password Authentication Scheme", Proceedings of ICCT, pp 1-5, 2013.

[9] Yair H. Diaz-Tellez, Eliane L. Bodanese, Theo Dimitrakos, Michael Turner, "Context-Aware Multifactor Authentication Based on Dynamic Pin", IFIP Advances in Information and Communication Technology, Volume 428, pp 330-338,2014.

[10] Kang, J., Nyang, D., Lee, K., "Two-factor face authentication using matrix permutation transformation and a user password", Information Science. 269, pp. 1–20, 2014.

[11] Cheong, Soon-Nyean, Huo-Chong Ling, Pei-Lee The, "Secure Encrypted Steganography Graphical Password Scheme for Near Field Communication smartphone access control system", Expert Systems with Applications 41.7, pp. 3561-3568, 2014.

[12] Khankari, Nilesh, and Geetanjali Kale, "Survey on One Time Password", International Journal of Computer Engineering and Applications, Volume 9, Issue 3, March 15