An Secure System Using Dynamic Password Based On Time And Date with Period Access

M. Vijay Akash[1], R. Siva Selvam[2], Mr.D.Shanmugavel[3], Mr. D. Rajinigirinath[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering,
[1, 2, 3, 4] Sri Muthukumaran Institute of Technology, Affiliated to Anna University, Chennai-25

Abstract- *In this research paper, time and date based dynamic password was presented to the overcome challenge of using a third party such as one-time password email, test and token device system for authentication in dynamic password authentication systems, user will set an user-id to how the password will be changing over a user-id with combination of date and time for each minute. We found that the system retains the strength of the dynamic password and improves the strength for password Attacks.*

Keywords- generations of dynamic password, two way authentication, time and date based dynamic password.

I. INTRODUCTION

The basic definition of a dynamic password is a password that does not remain the same, meaning it will constantly change. Passwords that are dynamically generated are based on an authentication method. It will send you a unique code that you must use once, expires within a short time period, and makes it more difficult for hackers to access your account. OTPs can be used by Google Authenticator and Microsoft Authenticator, both of which use OTPS to access the system, they will send you a 6-digit code you must use within one minute.

Password can be categorized in two:

A. ***Static Password:*** Is a type of password that does not change. An alphanumeric and special character combination is usually used to authenticate. This approach is vulnerable to key logging, brute force and dictionary attacks
B. ***Dynamic password:*** Is a type of authentication technique that the password changes. Dynamic password varies based of on the change factors and function, factor could be time lapse, or occurrence of an activity, function define how this factors take in the factors as parameters to change the accepted password at a particular time. This type of authentication uses a third party system to generate accepted passwords.

The static passwords are easier to recall compared to the dynamic passwords. A method for dynamically changing passwords based on a user defined pattern is proposed in this paper and the use of dynamic password without the need for third party systems

II. STATEMENT OFPROBLEM

The static passwords are easy to implementable and easy to use, but vulnerable to many threats such as keylogging, shoulder surfing, brute force attacks, etc., on the other hand the dynamic password tackle most of the threats faced by the static but accepted password at a particular time of authentication will have to be generated by some algorithm and made available to the user through unknown systems.

III. MERITS OFSTUDY

Using this research, security is improved by eliminating the use of third party systems and password attacks to generate a password and giving users the advantages of both the static and user-defined dynamic password systems.

IV. LITERATURE REVIEW

Security has a common issue in different industries when it comes to passwords. Today, many systems rely on static passwords to verify the identity of the user. [1] proposes a secure multimodal mobile authentication system using OTP. Most users use passwords that are easy to guess, repeat them in several accounts, and write them down. Others store them on their computer or somewhere else that is easily accessible.

A Time-based One-time Password through a secure tunnel was proposed by [2] A mobile app was developed for the project using TLS seed exchange and an offline encrypted keystroke. The objective of the research is to improve existing cryptographic standards and web protocols to design an alternative multi-factor authentication crypto system for the web. The system includes seed exchange to a software based token using a login protected transport layer security tunnel and an encrypted local storage through a keystroke that is password protected with a strong key derivation function and

offline generation of one-time passwords through the TOTP algorithm. Authentication is done through a shared secret (seed) to verify the accuracy of the OTP used for authentication.

A hybrid password scheme called T&C was proposed by [3]. In this system, multiple user authentication schemes are put together into a single scheme. The system is made up of alphanumeric characters and a location inside an image. Using the keyboard, users will enter the alphanumeric part of the password while location is identified using the mouse. The usability of this system is not a huge problem but passwords can be captured by online attacks. This is because they are directly used in the login screen.

An authentication system known called Pair Pass Char was proposed by [4]. The registration process of this system is the same as the registration process of the typical password method. In the login screen, all alphanumeric characters are displayed in a 10 by 10-grid format. In order to enter a password, the user has to logically search for rectangles that are formed by different pairs of password characters and then click on the corner characters of the rectangles. The system contains different rules for rectangle search thus making it difficult to learn. The average waiting time for six characters is 47.4 seconds which is veryhigh.
This access acquiring procedure is called Login [5].

V. METHODOLOGY

A. Algorithm: for Authentication.

*//**Title:** Dynamic Time Date Password*
*//**Input:** Time set (TS), Date Set (DS), Swap Section (SS), Input password (IP), System Password (SP), Unique Ref (UR)*
*//**Output:** correct password (Yes/No)*

IP+UR *user stamp*
SP+UR *system stamp*

IP+UR[SS] = 1/SP+UR
SP+UR[SS] = 1/IP+UR
TS+DS[IP]/2 = 0 Even(SS)
TS+DS[IP]/2 = 1 Odd(SS)

If (IP+UR SP+UR)
{
Return
{"Access Granted"}
Else
{"Access Denied"}
}

Other functions in the system are:

Reset: There is no reset time. It will automatically changes password for every minute.

Update: There is no changes until time changes. Update needs for user when they want.

VI. ANALYSIS

A. Proof of correctness:

Assuming a Input password(IP) as (12.09.2021)(12:02) and we want User Id (UR),Swap Section (SS)to be verify password by (IP) to(SP) for1minuteduration. From these verification, (IP) checks (SP) and (SP) checks (IP),If any one of these checks fails, the system will terminate. we can validate :

1) **Step1:**

Get values.
IP: (12.09.2021)(12:02),
SP: (12:02)(12.09.2021), UR: HH

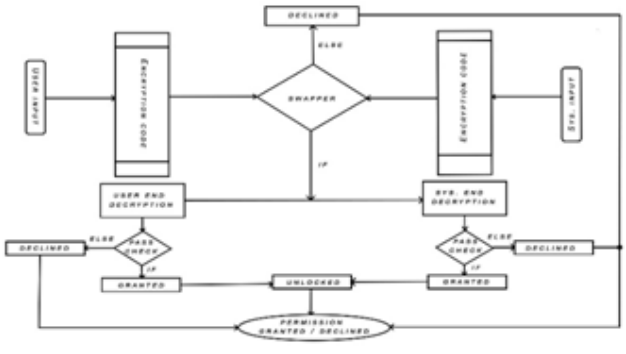
2) **Step2:**

Apply formula

IP+UR[SS] = 1/SP+UR
SP+UR[SS] = 1/IP+UR
IP+UR[SS] = 1/(TS+DS/2) + HH = HH+0 (Even)
SP+UR[SS] = 1/(TS+DS/2) + HH = HH+0 (Even)
IP+UR[SS] = 1/(TS+DS/2) + HH = 1+HH (Odd)
SP+UR[SS] = 1/(TS+DS/2) + HH = 1+HH (Odd)

IP+UR ← SP+UR

Note: *all values of password will use time and date with user id only.*



Note: *The stored password will not be the determining factor that will allow the user to gain access to the system. Rather, it will only be used as reference for getting the changing column and other values expected for a successful authorization. The function implemented in the code will be the determining value for authentication.*

VII. IMPLEMENTATION

In this section, we are going to discuss the implementing the algorithm defined. Implementation was carried for the windows platform.

Registration:

In order to use the application, the user will be required to enter their Unique ref. id. The System automatically assign dynamic procedure for user.

Login:

The login page allows users to login into their section. On successful Authentication, the user is given access to the secured data. On a three login attempts failed, the system will automatically enables second verification process for that user on the next access.

Forgotten password:

This application does not uses the forgotten password method through any options. User will wait for next minute for another access.

Tools used for the development are:

A. Software development tools

The software that was used for this development Visual studio. Visual studio was developed by Microsoft specifically for C# and .NET programming. It has a friendly environment that allows user to view and test their application as its being developed. The inbuilt SDK was used in order to run the application in order to debug errors.

B. Hardware tools

For any software to be developed, a hardware that will support the back and front end of the system is required. Below is the recommended hardware specification

VIII. RESULTS AND DATAANALYSIS

A. Methods of analysis

Research was carried out in order to find out the vulnerabilities/drawbacks of current authentication methods. Testing was done via surveys, interviews and observation by demonstration in order to know the level of usability, availability, reliability, speed and stability of the applications. Our population sample is50

Below are some of the important questions that were asked.

1. Would you prefer the system you just tested over DTDP?

Answer:30 of the people said they would prefer the new system. 10 of the people are not sure. And 8 of them have never used an DTDP method before.

Analysis:
We grouped them into 3 categories: Group A, B and C.
We made a calculation in order to find the percentage of each group.
Group A = 30
30/50 X 100 = 60%

Group B = 8
10/50 X 100 = 20%
Group C = 7
8/50 X 100 = 16%

This means that 60% of the people that were tested would go for the new implementation method. 20% are indecisive, and 16% have never used an DTDP before.

2. Would you prefer this system over static passwords considering that it has better security?

Answer: We got a 100% response on this question.

Their reason is that the system allows them to use their not guessable passwords but at the same time is secure because of its dynamic nature. At the same time, they can remember their password logic because the current password will be valid for one minute. And it will not predict.

In order to perform more test, we tested the popular authentication techniques against our new authentication method. The benchmarks below were used.

Benchmark	Usability	Availability	Reliability	Stability	Speed	Total
DTDP	1	1	1	1	1	5
User Defined Dynamic password	1	1	0	0	1	3
OTP	1	1	1	0	0	3
SMS and Email	1	0	1	1	0	3
Biometrics	1	0	1	1	1	4

Table 1: comparing existing system with the proposed system

The results show that our application is accepted because it does not require a device for password generation and is easy to be learnt.

1. **Usability**: People find it easy to use because the parameter required is not much. They prefer it over other methods because it does not require a device for authentication to occur.
2. **Availability**: The application is ready to be used at all times, because it does not require an email or SMS or device for correct code generation.
3. **Reliability**: The application is reliable because it always generates new password based on time and date parameters, and does not go out of sync.
4. **Stability**: The method is stable in the sense that it does not go out of synchronization and gives wrong passwords. In some cases, OTP's have gone out of sync. Users have to report to the administrator for a resync.
5. **Speed**: The system is fast to use because the parameters to remember for password authentication is not much, and one does not require to wait for a message or device to generate a correct password.

B. Attack possibilities

If we want to break their system, the user has to know certain factors. Changing logic, time date factor with correct order and unique reference ID or number. Without the knowledge of these factors, the attacker cannot break into the system.

IX. SUMMARY

From our data results and analysis, we have seen that our objective which is to improve static passwords has been achieved. Attacks such as phishing, key logging, and brute-force cannot work on our system.

X. CONCLUSION

In this research, we described DTDP, a simple and effective password method that generates a unique passcode for each minute. The calculation is based on both time and date. We also developed a simple prototype for windows using this DTDP. The implementation had the advantage of simple one-pass authentication, no need for a third party, low computation cost and no cost for proprietary tokens. However, using a mobile phone as the OTPs generator has vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks. We will try to counter these threats in future research.

REFERENCES

[1] R. McMillan, "Wired,"27 01 2012. [Online]. Available: https://www.wired.com/2012/01/computer- password/. [Accessed 9 102018].
[2] Uymatiao, L. T. Mariano and E. S. William, "Time-based OTP Authentication via Tunnel(TOAST): A mobile TOTP scheme using TLS seed exchange ad encrypted offline keystroke," 4th IEEE International Conference on Information Science and Technology(ICIST), pp. 225-229,2014.
[3] Subashini, K. Sumithra and G. , "Secure multimodal mobile authentication using one tome password," 2nd International Conference on Current Trends in Enginering and Technology (ICCTET), no. IEEE, pp. 151-155,2014.
[4] M. Akpulat, K. Bicakci and U. Cil, "Revising Graphical Password for Augmenting, not replacing text passwords," in 29th Annual Computer Security Applications,2013.
[5] Morris Robert and Ken Thompson, "Password security: A case history", *Communications of the ACM22.11*, 1979.