Time based Dynamic Password (TBDP) System using Variable Insertion Technique

Irshad Sharif Shaik
B. Tech, Computer Science and Engineering
ANU College of Engineering and Technology
Guntur, Andhra Pradesh, India

Mukkamala Manoj
B. Tech, Electrical and Electronics Engineering
K L University
Guntur, Andhra Pradesh, India

ABSTRACT
Nowadays most of the confidential works are carried under surveillance like Bank affairs, Research works, Enterprise projects etc. In this case, there is threat of capturing the confidential password of a user through surveillance cameras. Thesepasswords can also be captured through human surveillance (i.e. keen human observation) as well as a malicious program that run in background without user's knowledge. Serious problem arises if these confidential credentials go into wrong hands.Just typing the password in form of hidden characters does not avoid this problem. For this purpose, a security system has to be used that willprovide privacy to passwordseven under surveillance. Time based dynamic password system (TBDP) provides privacy to the user's login credentials by accepting varying password time to time. Password at particular time can't be accepted later.Users will be given privilege to define their own transformation logic using clock values that generates a time dependant password from a constant string (i.e. basic password declared by user).Here, transformation logic is based on variable insertion technique.At the time of login, users estimate their current password by collaborating the basic password and transformation logic defined over it and tries to login the system with those estimated credentials. Simultaneously, authentication system generates time varying password from Basic password and Transformation logic defined by user. Access is granted if the credentials are found to be valid at that time.In this way, this password system provides privacy to login credentials even under surveillance.

Keywords
Time Based Dynamic Password (TBDP), Transformation Logic, Variable Insertion Technique

1. INTRODUCTION
Time based dynamic password (TBDP) is a time varying password that is generated from a constant string (Basic Password) and Transformation Logic defined over it. This TBDP system helps to maintain confidentiality of login credentials even though someone has cracked the user's password. For example, if the user is using a password "abc123" at particular point of time. Some person has cracked this password using any of hacking techniques like phishing, background recording of system activities, surveillance cameras etc. Later, when the hacker tries to access the system using the same password, system denies the access as the password is dependent on time and time has changed. Accordingly, valid password also changes. In TBDP system, user defines his/her basic password as well as the logic that derives the time varying password from basic password. Complexity level of password lies in user's hand. User can choose the level of complexity basing on his/her requirement.

Basic password is string declared by user the time of credentials creation. This is similar to regular unchanging password we use.To add time dependant nature to basic password, we link it up with transformation logic that uses direct clock values (or) their respective functions. Transformation Logic is a function (or) a logic developed using clock values (minutes, hours, date etc.) to generate a time dependant password from basic password.Variable Insertion Techniqueis method of inserting variables into a string in specified positions. Transformation logic uses variable shift technique to insert variables derived from clock into basic password and generate time dependant variable password.

2. NECESSITY
Proper security maintenance should be provided to software applications in order to avoid unauthorized access. As to maintain privacy and confidentiality, software applications provide access to the users by verifying their unique credentials. If these credentials go into wrong hands, unfavorable results occur.So, users are supposed to keep their credentials in secret.

Surveillance is one of the techniques that help hackersto capture the credentials. Nowadays most of the confidential works like bank operations, enterprise projects etc., are carried under video surveillance. And these captured videos may become a tool for hackers to obtain credentials.Usage of hidden cameras is increasing nowadays. Serious problem will occur if our activities and operations are captured in the hidden cameras without our knowledge mainly targeted at time of credential usage. Which keys we are pressing in keyboard can be easily captured in these cameras. Not only the video surveillance, but the human surveillance too causes the same problem. If a person is keenly observing the keys which we are pressing at the time of password usage, there is chance that he can get our password that is being used. May be not in a single attempt, but he can succeed if he do this repeatedly. Nowadays new types of software are emerging that records what is happening in a system in detail. We can mention this as software surveillance. Without our knowledge our password may be captured with help of software surveillance too.

As to avoid all these problems, a security system has to be developed that avoids unauthorized access even though our password is captured. This can bedone by accepting the password that varies time to time. If someone captures our password at particular time, then that password will be of no use in later time, as the valid password at that time will be different. The users will be known with the logic how their passwordis changing time to time.TBDP system mainly works basing on varying credential technique (i.e. Transformation Logic)that is developed using time elements. So, there is

necessity of this kind of security system in the current technical world.

3. WORKING

Working of TBDP depends on Transformation Logic.At the time of account creation i.e.at the time of password creation, Users have to define their own transformation logic. This transformation logic uses variable insertion technique while generating the time dependant variable password.

User should define his transformation logic using time variables like year (**y**), month (**m**), date (**d**), hour (**h**) and minute (**min**). User can also include functions of these time variables like (**y+1**), (**2m**),(**h%10**), (**h+m**) etc. Along with these time elements, user has to choose their positions to insert them within the basic password. This method of inserting the variables within the string is referred as Variable Insertion Technique.Basic password and time variables along with the details of their positions are stored in database. As the time change, values of time elements changes. Accordingly, the string generated by combining time elements and basic password also changes. This is how the varying nature is added to passwordin TBDP.

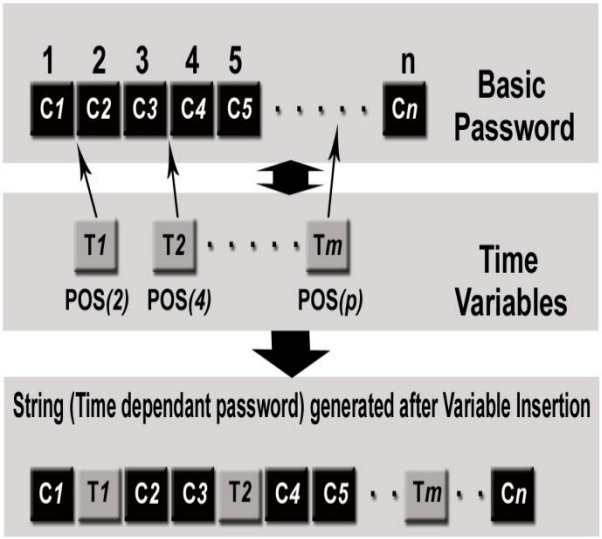

Fig 1.Variable Insertion Technique.

Consider an example, let the basic password defined by user is "abcd" and the selected time elements are **h** in position 1and **min** in position 3. Now the general form of password will be like "**h**ab**min**cd" where **h** is hour value replacement in position 1 and **min** is minute value replacement with position 3. If the current time is 10:42 then present valid password will be "10ab42cd". Similarly, if the time is 22:30, then password valid at that time will be "22ab30cd". When user wants to access the system, however, he would be known with his basic password and the positions where to insert the time elements; he estimates the password by inserting time element within the basic password in the positions he had choose and use that estimated password as the login password. At the same time, authentication system retrieves basic password and details relating to time variables from database and generates the current valid password. Access to system is granted if the user's estimated password and time dependant password generated by system matches. Even the basic password is also considered as invalid password. It is treated to be valid only when it is integrated with time elements.

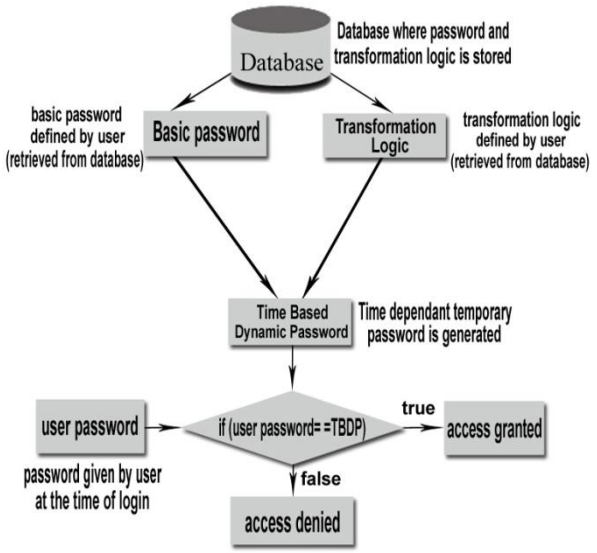

Fig 2. Implementation of TBDP

4. RELATED WORKS

4.1 Time based Dynamic password System using ASCII Shift technique

This is password system where time dependant password is created using ASCII Shifttechnique in transformation logic. ASCII Shift is a method of adding certain value to ASCII values of characters in a string to generate a new string. Transformation logic is build using time elements to generate a time dependant factor called Transformation Factor (F_t). This F_t value is used by ASCII Shift technique to generate a new string (i.e. time dependant password) from basic password.

Implementation of ASCII Shift technique is as follows:

functionasciiShift (array[ ] ascii_basic_password, number F_t)
{

array[ ] ascii_tbdp;

// array to store new ASCII values

for(number i=0; i<length_of (ascii_basic_password); i++)

{

ascii_tbdp[i] = ascii_basic_password [i] + F_t ;

// transforming the ASCII values of basic password

}

returnascii_tbdp; }

For more details regarding to Time Based Dynamic Password Using ASCII Shift Technique refer to article [1].

4.2 One Time Password

One Time Password (OTP) [2] is a technique in which user is provided with randomly generated password that is valid for only a small time. Using this password later will be of no use. This system is implemented with the help of additional hardware device like mobile phone. One time password technique is implemented in mobile phone by sending the login password in form of text message. One time password technique is also implemented using some other devices namely Security token, USB tokens, Cryptographic tokens that displays the password on a digital display available in the

device at the time of login. This method provides good responsive mechanism for many types of security attacks. But, this method does not provide a better solution when the additional hardware or external device used by this technique is lost or theft by someone intentionally. Proper maintenance of additional devices is also mandatory to implement this technique in efficient way.

5. RESULTS AND DISCUSSIONS

5.1 Applications

- TBDP system can be implemented in the places where confidential projects carry on. And it can also be used in secured activities like bank transactions to further increase the level of security and privacy to users.
- This system can be implemented in high level security management devicesdeployed for the valuable things like antiques, defense tools, confidential documents etc.
- This system can also utilized by officials in high level cadre of an enterprise to further improve the quality of security and privacy to their credentials.
- TBDP system can be implemented in cyber based applications to keep our credentials protected from unethical cyber trackers.

5.2 Advantages

- As valid passwords are not directly stored in database, this increases the level of security to the credentials maintained by an application.It also protects the credentials stored by anapplication from malicious hacking sources [3].
- TBDP System protects the credentials of user from various types of surveillance like Video surveillance, Human surveillance and Software surveillance.
- TBDP system reduces the chances of Brute-force attack [4], Dictionary method [5] and various kinds of credential cracking techniquesto succeed.

6. CONCLUSION

As there is rapid increase in security threats for software based operations, there should also be an improvement in the quality of security provided. Preventive measures have to be taken to avoid unethical hackers to succeed in their intension and causing a great damage. Implementation of TBDP system will improve the level of security and privacy to user credentials. TBDP system also helps the users to use his credentials without the fear of surveillance.

7. REFERENCES

[1] Irshad Sharif Shaik, IJERT December Issue, 2014: Time Based Dynamic Password Using ASCII Shift Technique.

[2] R. J. Barlow, A. R. Barnett. John Wiley & Sons, 1998. Computing for Scientists: Principles of Programming with FORTRAN 90 and C++.

[3] Cameron H. Malin, Eoghan Casey, James M. Aquilina. Malware Forensics: Investigating and Analyzing Malicious Code.

[4] Klaas Apostol. Salupress, 2012. Brute-Force Attack.

[5] Seymour Bosworth, Michel E. Kabay, Eric Whyne. John Wiley & Sons, 2014. Computer Security Handbook 6th edition.

[6] David Salomon, Springer Science & Business Media, 2003. Data Privacy and Security: Encryption and Information Hiding.

[7] Mark Ciampa. Cengage Learning, 2008. Security+ Guide to Network Security Fundamentals Cyber Security Series.