International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

Time Based Dynamic Password (TBDP) System using ASCII Shift Technique

Irshad Sharif Shaik
B.Tech, Computer Science & Engineering
ANU College of Engineering and Technology
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 secret credentials of a user in surveillance cameras. These credentials can also be captured with the help of human surveillance and installation of malicious programs too. Serious problem may arise if these credentials go into wrong hands. Just typing the secret credentials (i.e. password) in the form hidden characters do not avoid this problem. For this purpose, a security system has to be used to provide privacy of credentials even under surveillance. Time based dynamic password system (TBDP) provides privacy to the user by accepting the varying credentials time to time. Credentials at this time cannot be accepted later. User will be known with transformation logic that generates the transformation factor, basing on which the valid password changes time to time using 'ASCII Shift' technique. Transformation logic can also be defined by user using time elements like date, hour, minute and so on at the time of credentials creation. In this way, this password system provides privacy even under surveillance.**

Keywords: Time Based Dynamic Password (TBDP), Transformation Logic, Transformation Factor, ASCII Shift.

I. INTRODUCTION

Security threats are increasing day by day in the field of software technology. Software applications are playing prominent role in current society activities like business, banking etc. Cyber based applications are also having a growing importance. Even though there is day to day increase in the quality of security, the hackers are developing their hacking techniques too. Surveillance will become helping hand to these credential crackers. Surveillance may be video surveillance, human surveillance, software surveillance etc. All these techniques may help the hackers to succeed in their unethical intension. So, the Time Based Dynamic Password (TBDP) system is being developed to provide security from these surveillance threats. 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. Overall implementation of TBDP is considered as TBDP System. Transformation Logic is logic (or) function developed using time elements that generate a factor namely 'Transformation Factor' that varies according to values of time elements mentioned in it. Transformation Factor is the value resultant of Transformation Logic when the time elements are substituted with their current values. And this Transformation Factor is further used in ASCII Shift technique (*discussed in later sections*) to generate a time varying password. Implementation of TBDP involves the integration of Basic Password, Transformation Logic and ASCII Shift technique and their collaborated working. Software applications are mostly frightened by the hacking techniques like Brute-force method, Dictionary Attack etc. TBDP system also reduces the chances of these hacking techniques to succeed. Hence the implementation of this TBDP will keep the security management technologies ahead from these threatening technologies.

II. 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 user by verifying their unique credentials. So, users are supposed to keep their credentials secret. If these credentials go into wrong hands, unfavorable results may occur. Surveillance is one of the techniques that help hackers to capture the credentials. Now-a-days 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 now-a-days. 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. Not only the video surveillance but the human surveillance too causes the same problem.

Now-a-days 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 credentials 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 credentials are captured. This can be done by accepting the credentials that vary time to time. If someone captures our credentials at particular time, then that credentials will be of no use at later time, as the valid credentials at that time will be different. The user will be known with the logic how his credentials changes time to time and hence, capturing

credentials at some time will be of no use. Likewise, the privacy for user credentials will increase with the help of this varying credential technique. TBDP system mainly works on the basis of this varying credential technique basing on the logic developed using time elements. So, there is necessity of this kind of security system in the places where the works basing on software applications are carried under surveillance.

III. WORKING

Working of Anti surveillance security system is not much complicated. It works as traditional authentication system, but importance is given to transformation logic that generates varying credentials. At the time of account creation *i.e.* At the time of credentials creation, Users have to define their own transformation logic or else they have to choose one of the predefined logics provided. This transformation logic generates a transformation factor. And this transformation factor is used to generate a time dependant variable password using ASCII Shift technique. This basic password and transformation logic relating a particular user are considered as strings and stored in database in encrypted form [4] if required.

User evaluates the login credentials at particular time by applying the transformation logic on basic credentials, and requests the access with those credentials. Then the system captures both basic password and transformation logic of user from database and substitutes the time elements in transformation logic to generate a transformation factor. Basing on the transformation factor, a time dependant temporary password is generated using ASCII Shift technique. Then TBDP system compares the temporary password generated by system and the password given by user. If both matches access is granted to user else, access is denied. User is not given access until he gives proper credentials as input. Even the direct usage of basic password is not allowed. Only, the evaluated time dependant password is accepted by TBDP system.

Working of TBDP system is based on two elements :

A. Transformation Logic

Transformation Logic is a function developed using time elements to derive Transformation Factor. Time elements include year value, month value, date value, hour value and minute value. As the time variables changes frequently, resulting value of transformation factor changes accordingly. Here is generalized form of Transformation Logic

$$F_t = a.\ year(t) + b.\ month(t) + c.\ date(t) + d.\ hour(t) + e.\ minute(t) \quad (1)$$

- F_t = Transformation Logic ;
- *year(t)* = Current year value in clock;
- *month(t)* = Current month value in clock;
- *date(t)* = Current date value in clock;
- *hour(t)* = Current hour value in clock;
- *minute(t)*= Current minute value in clock;

a, b, c, d, e are constant integer values

For example, If the current clock time is 01:05:43 AM, 11/27/2014 (mm/dd/yyyy).Then *year(t)*=2014; *month(t)*=11; *date(t)*=27; *hour(t)*= 01 ; *minute(t)*= 05 ;

Let us consider an example of Transformation Logic where a = 0; b = 0; c = 0; d = 2; e = 1; (defined by user at the time of account creation) then $F_t = 2.hour(t) + 1.minute(t) = 2.(1) + 1.(5) = 7$; $F_t = 7$;

This transformation factor is factor used in ASCII Shift technique to generate time dependant temporary password.

B. ASCII Shift Technique

ASCII [5] stands for American Standard Code for Information Interchange. ASCII value [5] is a unique integer associated with every character. ASCII Shift is a technique of shifting ASCII value of character to a certain value. In TBDP System ASCII Shift technique is used to change the ASCII values of characters in basic password by adding Transformation Factor to current ASCII value of every character in it. Then, A new string is formed basing on changed ASCII values. And this new string is considered as temporary valid password.

Consider the same example of Transformation Logic as mentioned in previous section. Here the Transformation Factor (F_t) obtained is '7'. Let us consider basic password defined by user as "ABCD" whose ASCII form is 65-66-67-68. When user request for access, Basic password is retrieved from database and ASCII Shift is performed basing on transformation factor. Then valid temporary password generated is "HIJK" (72-73-74-75) *i.e.* value of 7 is added to previous ASCII values ((65+7)-(66+7)-(67+7)-(68+7). TBDP System checks whether the password given by user and temporary password generated by system matches or not. If both match, access is granted. Else, access is denied. User should give 'HIJK' as password instead of 'ABCD' (Basic Password) to acquire access over the system he required.

Implementation of ASCII Shift technique is as follows:

```
function asciiShift (array[ ] ascii_basic_password, number Ft ) {
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 ] + Ft ;
// transforming the ASCII values of basic password
}
return ascii_tbdp;  }
```

To provide simplicity users will be given an option to choose some predefined simple transformation logics. Else, they can define their own transformation logic. Basing on the requirement, they can choose their own level of complexity. Transformation logic can also be included with operations on time elements like multiplication, subtraction, squares etc. User should be cautious before defining Transformation logic as resulting Transformation Factor may cross limits sometimes and increases complexity.

IV. RELATED WORKS

A. One Time Password

One Time Password (OTP) [6] 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 within the device at the time of login. This method provides good responsive mechanism for many types of cracking attacks. But, this method does not provide a better solution when the additional hardware or external devices used by this technique are lost or theft by someone intentionally. Proper maintenance of additional devices is required as to implement this technique in efficient way.

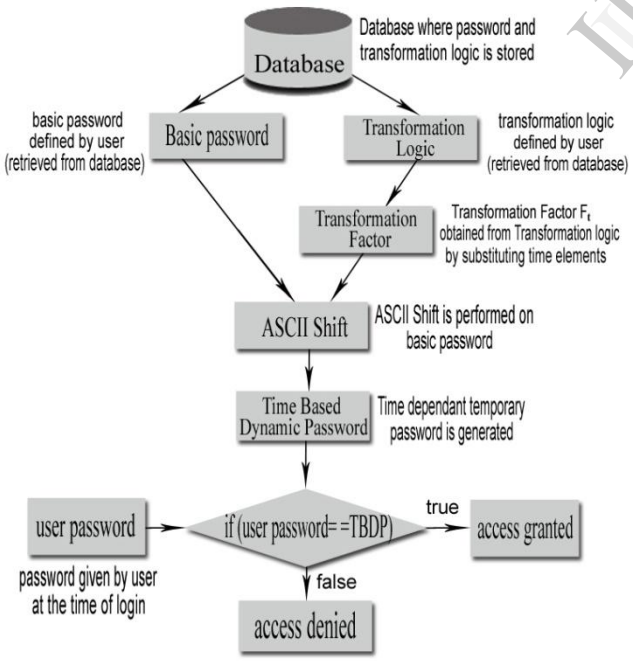

Fig. 1. Working of anti-surveillance security system

V. RESULTS AND DISCUSSIONS

A. Applications

- TBDP system can be implemented in the places where confidential projects will carry on. And, it can also be used in secured activities like bank transactions as to further increase the level of security and privacy to users.
- This system can be implemented in high level security management 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.

B. Advantages

- As valid passwords are not directly stored in database, this increases the level of security to the huge number of credentials maintained by an application.
- 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 [2], Dictionary method [3] and various kinds of credential cracking techniques to succeed.
- It also protects the credentials stored in application from malicious codes [1].

C. Safety Measures

- Users should be careful about their basic password and transformation logic implemented. They should not reveal it to others in any case.
- To avoid complexity, users have to design a transformation logic in such a way that the resulting credentials would stay within a certain limit. Otherwise it will increase the complexity.
- As to include alpha-numeric symbols in this system, it is better to provide user with basic information about ASCII values.

VI. OWN WORK

A successful implementation of TBDP system has done and we are working for the advancement of TBDP System. We are putting forth the idea *TBDP using Variable insertion Technique* that adds simplicity to the TBDP System by eliminating the complex calculations of ASCII values involved in "TBDP using ASCII Shift Technique". This adds simplicity and convenience to users to use this kind of high privacy security system.

VII. 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.

REFERENCES

1. Cameron H. Malin, Eoghan Casey, James M. Aquilina. Malware Forensics: Investigating and Analyzing Malicious Code.
2. Klaas Apostol. Salupress, 2012. Brute-Force Attack.
3. Seymour Bosworth, Michel E. Kabay, Eric Whyne. John Wiley & Sons, 2014. Computer Security Handbook 6th edition.
4. David Salomon, Springer Science & Business Media, 2003. Data Privacy and Security: Encryption and Information Hiding.
5. R. J. Barlow, A. R. Barnett. John Wiley & Sons, 1998. Computing for Scientists: Principles of Programming with Fortran 90 and C++.
6. Mark Ciampa. Cengage Learning, 2008. Security+ Guide to Network Security Fundamentals Cyber Security Series.