Research Inventy: International Journal Of Engineering And Science
Vol.2, Issue 10 (April 2013), Pp 14-17
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology

[1,]Ms. E.Kalaikavitha M.C.A., M.Phil., [2,]Mrs. Juliana gnanaselvi M.Sc., M.Phil., Ph.D.,

[1,]*Asst. Professor, Dept. Of Information Technology. Rathinam College Of Arts And Science College. Coimbatore-21.*
[2,]*Head Dept Of Information Technology, Rathinam College Of Arts And Science College. Coimbatore-21.*

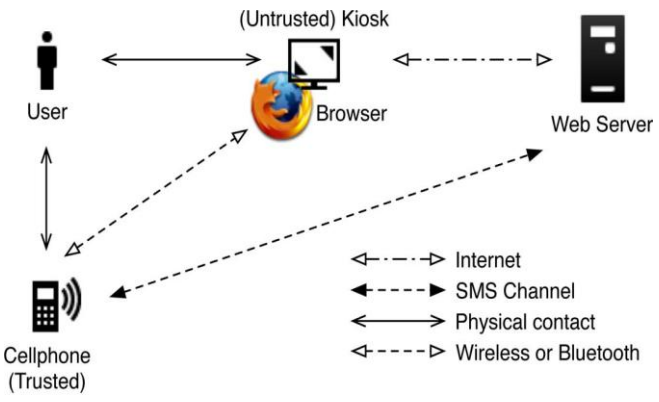
Abstract: *In Online based applications most of them used static passwords. In that they follow multiple technics to secure their credentials. For examples: Multi level password authentications, hard codes, Session Passwords, bio- matric technics, and One Time Password. Every method has some advantages and disadvantages. Our proposed idea is to enhance the security level of One Time Password by Encrypting it and logging the user by forwarding the encrypted OTP with Password to the system. It increases the security level of the system.*

Keyword*: Static Password, One Time Password, Encrypted OTP, Mobile based login,*

I. INTRODUCTION:

In Online based Application having few main advantage and many disadvantages when it comes to weak single-factor authentication, which many are more familiar with as the single static passwords still employed by most companies. One advantage is that static passwords are easy to remember. However, when different systems have different passwords, they can be difficult to remember and may have to be written down, raising their vulnerability. The many disadvantages of single static passwords include how easy they are to decipher. Most often, they are short and based on subjects close to the user—birthdays, partner names, children's names—and they are typically only letters.

Single static passwords are also vulnerable to social engineering, i.e., people asking for passwords or guessing them correctly. Some surveys carried out at railway stations have shown how easy it is to get people to reveal their passwords. They can also be picked up by spyware. It is having many chance to others can accessing their personal accounts, otherwise we need to change the password repeatedly. To overcome these drawbacks new method is invented that is called "One Time Password (OTP)". OPT is a password that is valid for only one login session or transaction. This OPT allow the user to get login into the system by entering their password with OTP. In our proposed approach is, after user entering the username and password web server generates the Encrypted OTP using AES algorithm and send it to the users mobile. OTP is an encrypted format, so users can't read it. Instead of that, user needs to forward that OTP with system logging password to the system. At the system end encrypted OTP is decrypted and verify the OTP, Password and mobile number for a particular username.in this approach user's information are verified in many levels. It avoids the unauthorized logging. The process of secure login using encrypted OTP with mobile based logging model is shown in following figure:



II. STATIC PASSWORD:

The impact of the Internet over the last few years has meant fundamental changes in the way we access business systems. The network security perimeter has crumbled at all levels while the number of users wanting network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world. While there are enormous productivity benefits available from increased access, the security risks have greatly increased. The traditional method of securing system access was by authentication through the use of passwords.

Unfortunately, traditional password authentication is totally unsuitable for securing the access requirements of today's distributed users. According to the DTI Information Security Breaches Survey 2006, businesses are still overwhelmingly dependent on user IDs and passwords to check the identity of users attempting to access their systems. Weak single factor authentication is the use of single static passwords and still employed by most companies. The benefit is that static passwords are easy to remember. However, when you have different passwords for different systems, they start to become very difficult to remember and have to be written down, making them vulnerable. The many disadvantages of single static passwords include how easy it is to crack them. They are short and based on topics close to the user, such as birthdays, partner names, children's names, etc; and they are typically letters only. They are also vulnerable to social engineering i.e. people asking for your password or guessing it. They can also be picked up by spyware.The alternative method of password management is to change passwords regularly. Operated correctly, this has the benefit of being more inherently secure than static passwords. A disadvantage of frequently changing passwords is that they can be easily forgotten, leading to very high support costs and significantly increased administration costs. This is particularly relevant for larger organizations with hundreds of applications.

2.1 One Time Password (OTP):

A **one-time password** (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

How to generate OTP and distribute?

OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on **time-synchronization** between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical **algorithm** to generate a new password **based on the previous password** (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical **algorithm** where the new password is **based on a challenge** (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

2.2 Methods of generating the OTP

Time-synchronized

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source. An example of time-synchronized OTP standard is TOTP.All of the methods of *delivering* the OTP below may use time-synchronization instead of algorithms.

2.3 Mathematical algorithms

Each new OTP may be created from the past OTPs used. An example of this type of algorithm, credited to Leslie Lamport, uses a one-way function (call it *f*). The one-time password system works by starting with an initial seed *s*, then generating passwords

f(*s*), *f*(*f*(*s*)), *f*(*f*(*f*(*s*))), ...

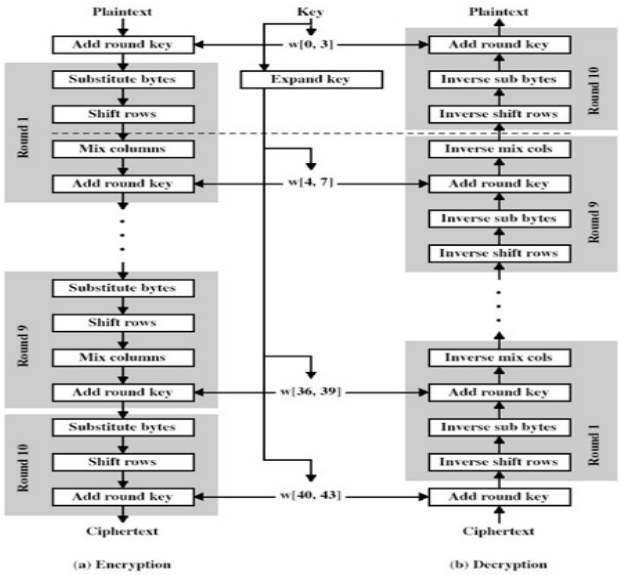
as many times as necessary. Each password is then dispensed in reverse, with *f*(*f*(...*f*(*s*))...) first, to *f*(*s*). If an indefinite series of passwords is wanted, a new seed value can be chosen after the set for *s* is exhausted. The S/KEY one-time password system and its derivative OTP are based on Lamport's scheme.An intruder who happens to see a one-time password may have access for one time period or login, but it becomes useless once that period expires. To get the next password in the series from the previous passwords, one needs to find a way of calculating the inverse function f^{-1}. Since *f* was chosen to be one-way, this is extremely difficult to do. If *f* is a cryptographic hash function, which is generally the case, it is (so far as is known) a computationally infeasible task.In some mathematical algorithm schemes, it is possible for the user to provide the server with a static key for use as an encryption key, by only sending a one-time password.[1]The use of challenge-response one-time passwords requires a user to provide a response to a challenge. For example, this can be done by inputting the value that the token has generated into the token itself. To avoid duplicates, an additional counter is usually involved, so if one happens to get the same challenge twice, this still results in different one-time passwords. However, the computation does not usually involve the previous one-time password; that is, usually this or another algorithm is used, rather than using both algorithms.The methods of delivering the OTP which are *token-based* may use either of these types of algorithm instead of time-synchronization.

III. ENCRYPTED OTP:

Generated OTP value is encrypted using powerful AES algorithm and sends it to users.

AES algorithm: AES is an iterative and a symmetric key block cipher that uses three keys strengths of 128, 192 and 256 bits. The AES encryption and AES decryption occurs in blocks of 128 bits. The maximum block size can be 256 bits however the key size has no theoretical maximum. Unlike the public key ciphers the AES cryptography uses the same key to encrypt and decrypt data. The user simply need to select AES encrypt or AES decrypt and the encryptor will do the rest. It is one of the perfect cryptography algorithms to protect personal data. The encrypt AES tool converts the input plain text to cipher text in a number of repetitions based on the encryption key. The AES decrypt method uses the same process to transform the cipher text back to the original plain text using the same encryption key.AES has also been called Rijndael on its inventors Joan Daemen and Vincent Rijmen. It was issued by US Government's National Institute of Standards and Technology (NIST) in 1997. It is one of the strongest encryption methods that are hard to break. The hash is used to protect the encryption key against brute force attack. It is being used to secure online information, financial transactions by banks, e-commerce sites and other financial institutions.

Process of AES algorithm shown below:
The encrypted OPT password is send to mobile through Bluetooth technology or modem.



IV. MOBILE BASED LOGIN METHODOLOGY:

In mobile based technology user no need to enter OTP manually, because of security reasons OTP is encrypted and sends to mobile. User just read the mail for verification and type application password with that encrypted OTP and sends it to the system Web server is used to send mail to user. In this technology others can't try to enter OTP, if others can mean they don't know the application password. Using this we can verify users OTP, Password and mobile number also. It provides the highest level of authentication for the system

V. CONCLUSION:

In this paper, we have proposed a new idea to enhancing the performance of the One Time Password to provide Authentication for System. OTP is encrypted and send to user and user can login only using mobile based technology. This approach provides the high level authentication to the system by verifying the user's Password, OTP and mobile number. In this method somewhat system load is increased by encrypting and decrypting of OTP for multiple users. In the future, we plan to study how to reduce the system load and increase system performance while using this approach.

REFERENCES:

[1] V. A. Brennen. (2004). Cryptography Dictionary, vol. 2005, 1.0.0 ed. [Online]. Available: http://cryptnet.net/fdp/crypto/crypto-dict/en/crypto- dict.html
[2] M. Abadi, L. Bharat, and A. Marais, "System and method for generating
[3] unique passwords," U.S. Patent 6 141 760, 1997.
[4] [Online]: research.microsoft.com/apps/pubs/default.aspx?id=132349
[5] **[**Online]:www.slideshare.net/ttnjal/200804NISnetNFCNoll