International Journal Of Advanced Research In Engineering Technology & Sciences
ISSN: 2394-2819
Email: editor@ijarets.org March- 2015 Volume 2, Issue-3 www.ijarets.org

Password Management Using OTP Authentication

Anand Pandey
Assistant Professor
Department of Information Technology
SRM University
Modinagar, Ghaziabad

Saurabh Nair, Satyam Sharma, Manav Mehta
B Tech Students
Department of Information Technology
SRM University
Modinagar, Ghaziabad

ABSTRACT
Passwords, itself means an increased layer of security that helps a user log into his various social networking sites or even accesses his net banking facilities by a simple authentication password created by the user himself. But the passwords created by user is not always that secure or safe. Moreover, it is not tedious task for out brain to remember all such complex passwords. So here we have designed a combined schema for managing the passwords of the user with the help of OTP authentication concatenated with an alphanumeric master password. This designed model thus makes uncomplicated to commit to memory and it is also computationally powerful.OTP algorithm makes a finite alphanumeric token valid for a session and for a single use.Our password manager provides an easy way of system authentication schema which enables the user not obligatory to memorize any difficult passwords or character combinations. Concatenation of the OTP authentication and the password manager not only increases usability but also makes it almost impossible to break such password managers or other attacks like brute force attacks.

Keywords: OTP, Authentication, password, management

I. INTRODUCTION

Passwords are the main way we identify ourselves online. They have been essential to the security of our personal information as well as that of large corporations. From Face book to bank accounts, we rely on passwords for almost every type of service we use, but it's becoming increasingly hard to maintain and protect them all. Now innovative technologies are attempting to turn our bodies and even our behaviour into the ultimate protectors of our personal data. Increasing dependence on passwords has led us to develop new software which has multiple security layers.

It will be a desktop application mainly written in JAVA and with an increased security layer of OTP authentication which will ensure a secure log in of the registered users. The most important advantage 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. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

OTP as one layer in layered security is safer than using OTP alone; one way to implement layered security is to use an OTP in combination with a password that is memorized by the user (and never transmitted to the user, as OTPs often are). An advantage to using layered security is that a single sign-on combined with one master password or password manager becomes safer than using only 1 layer of security during the sign-on, and thus the inconvenience of password fatigue is avoided if one usually has long sessions with many passwords that would need to be entered mid-session (to open different documents, websites, and applications)

In this research we will look at novel alternatives to passwords and try to glimpse into the future of personnel identification and also ensures the easy management of all social networking sites including the storage of credit card/debit card PINs and other important passwords.

II. PASSWORD MANAGEMENT

Password management is a way to organise and save your important passwords at a single location which can be solely accessed by the user only. There has been a lot of password theft incidents in the recent past which has to led to the development of such password management software.

Users often have many different computer accounts at work, for their cell phone, at their bank, with insurance companies, and so on. To make it easier to remember their passwords, users often use the same or similar passwords on each system; and given a choice, most users will select a very simple and easy-to-remember password such as their birthday, their mother's maiden name, or the name of a relative.

Short and simple passwords are relatively easy for attackers to determine. Some common methods that attackers use for discovering a victim's password include:

- Guessing-The attacker attempts to log on using the user's account by repeatedly guessing likely words and phrases such as their children's names, their city of birth, and local sports teams.
- Online Dictionary Attack-The attacker uses an automated program that includes a text file of words. The program repeatedly attempts to log on to the target system using a different word from the text file on each try.
- Offline Dictionary Attack-Similar to the online dictionary attack, the attacker gets a copy of the file where the hashed or encrypted copy of user accounts and passwords are stored and uses an automated program to determine what the password is for each account. This type of attack can be completed very quickly once the attacker has managed to get a copy of the password file.
- Offline Brute Force Attack-This is a variation of the dictionary attacks, but it is designed to determine passwords that may not be included in the text file used in those attacks. Although a brute force attack can be attempted online, due to network bandwidth and latency they are usually undertaken offline using a copy of the target system's password file. In a brute force attack the attacker uses an automated program that generates hashes or encrypted values for all possible passwords and compares them to the values in the password file.

III. OTP IN PASSWORD MANAGEMENT

One Time Password Security System & Tokens such as Secure OTP Authentication Server 3 by Secure Metric Technology uses One-Time-Password (OTP) technology to provide strong authentication. An OTP is a password that is valid for only ONE login session or transaction and after that it becomes obsolete. It is also known as a dynamic password. There are two approaches to generate an OTP:

Time based OTP – the OTP changes at frequent intervals (for example every 30 or 60 seconds).

Event-based OTP – the OTP is generated by pressing a button on the OTP device or token.

- Time based OTP – the OTP changes at frequent intervals (for example every 30 or 60 seconds).
- Event-based OTP – the OTP is generated by pressing a button on the OTP device or token.

A. OTP Authentication

Each password is ungues sable, even when previous passwords are known. The open source OATH algorithm is standardized; other algorithms are covered by U.S. patents. Each new password is unique, so an unauthorized user would be unable to guess what the new password may be, based on previously used passwords.

A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that will authenticate the user for a single transaction or session.

B. OTP generation

The OTP provider makes use of randomness and pseudo randomness and also hash algorithm making it impossible for the attacker to predict the password. The use of hash algorithm necessary because it then creates a random OTP every time a user wants it instead of creating the ones that can be predicted on the basis of the previous ones.

Various ways to generate OTPs are listed below:

- **Time-based** OTP authentication between the server and the client providing the password. Here the password is available only for a short period of time.
- A mathematical **algorithms** often used 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

Different ways for Delivering OTPs:

- Message based
  It is the most common way of delivering the OTP to the respective user. Basically, it is the most accessible means for the delivery of the OTP as it is the most ubiquitous communication channel and is available on almost all the mobiles. Thus, text messaging has a great potential to reach all consumers with a low total cost to implement.

- Mobile phones
  A mobile phone keeps costs low because a large customer-base already owns a mobile phone for purposes other than generating OTPs. The computing power and storage required for OTPs is usually insignificant compared to that which modern camera-phones and smartphones typically use. Mobile phones additionally support any number of tokens within one installation of the application, allowing a user the ability to authenticate to multiple resources from one device. This solution also provides model-specific applications to the user's mobile.

- Web-based
  Authentication-as-a-service providers offer various web-based methods for delivering one-time passwords without the need for tokens. One such method relies on the user's ability to recognize pre-chosen categories from a randomly generated grid of pictures. When first registering on a website, the user chooses several secret categories of things; such as dogs, cars, boats and flowers. Each time the user logs into the website they are presented with a randomly generated grid of picalphanumeric character overlaid on it. The user looks for the pictures that fit their pre-chosen categories and enters the associated alphanumeric characters to form a one-time access code.

IV. EXISTING TECHNOLOGY

We studied some of the already existing password managing software and some of the studied machines are:

1. 1Password
   1Password is a comprehensive password manager developed by AgileBits Inc. It provides a place for users to store various passwords, software licenses, and other sensitive information in a virtual vault that is locked with a PBKDF2-guarded master password.

2. Dash lane
   Dash lane is a password manager app and secure digital wallet that provides solutions to the problem of password fatigue. The app is available on Mac, PC, iOS and Android, The app's premium feature enables users to securely sync their data between an unlimited numbers of devices on all platforms.

3. Password Safe

Password Safe is a free and open-source password manager program for use with Microsoft Windows. A beta, command-line, version is also available for Ubuntu (including the Kubuntu and Xubuntu derivatives) and Debi an operating systems. A Java-based version is also available on Source Forge. On its page you can find links to unofficial releases running under Android, BlackBerry and other mobile OS.

These are few password managers that are considered to be the best in the world. But we found that even the best of the password managers can be unsafe and hacked using hacking attacks like brute force attacks and other hacking attacks. This happens mainly because of the old styled password generator that can always be calculated using some algorithms.

V. PROPOSED TECHNOLOGY

Today most enterprise networks, e-commerce sites and online communities require only a user name and static password for logon and access to personal and sensitive data. Although this authentication method is convenient, it is not secure because online identity theft – using phishing, keyboard logging, man-in-the-middle attacks and other methods – is increasing throughout the world.

After analyzing and understanding the existing technologies, we decided on developing a password manager that cannot be hacked and has a multilayered security as its master password in the system by using One Time Password generation.

Our proposed technology edges over the existing technologies because of the use of instantaneous passwords in our password manager which will provide an increased security layer to the users.

No password manager until now have used OTP authentication in their system, thus it is the first attempt on such technology. In this we will be using a finger print scan machine for the master password authentication unlike the other existing technologies where we were using old fashioned passwords for master password which ultimately increased complexities.

In our proposed model, we will providing the following features:

- Authentication using the OTP authentication as a primary master password and other password as the secondary master password.
- Storage of all important passwords like passwords of important websites like face book, Gmail, linked in, twitter, yahoo, flip kart, eBay etc.
- Provision of storing and managing credit card/debit card PINs and other important passwords.
- Use of OTP technology to store other useful important information, documents etc.

VI. RESULTS

The proposed model has been tested and implemented successfully and thus all the codes and the API communication was efficiently executed. Thus, the higher strengthen security measure of OTP when it added with proper Password. This highest measure cannot be predicted and not to be traced by malwares and other possible passive and active attacks. At the same time, it is relatively fastest authentication scheme for secure networks.

An iterative form of testing was performed on the developed model to make it free from all the possible errors and bugs. It was effectively carried out by our team with profound results. The code snippets and the algorithm were checked for syntactical and logical mistakes using proper testing methods. The IDE environment also gave us the expected results when the program was executed. The use of database developer MySQL for executing the queries was also tested successfully and henceforth successfully managing the databases for storing information like user ID, password and the dynamic OTP that is entered and saved into the database every time an OTP was generated.

In this research and designed work, it was observed that the password manager worked successfully with the entire windows platform that had pre-requisite java environment (jdk 1.6). Thus, it can be collectively said that the development of the software using JAVA and My SQL database was successful and then connecting the software to an OTP environment using the available APIs was also successful.

VII. REFERENCES

1. Yi-Bing Lin Meng-Hsun Tsai Nat. Chiao Tung Univ., Hsinchu "Eavesdropping Through Mobile phone" IEEE Transactions on Vehicular Technology Volume:56 Issue:6 on pages: 3596 – 3600.
2. Callegati, F. Cerroni, W. Ramilli, M. Univ. of Bologna, Bologna "Man-in-the-Middle Attack to the HTTPS Protocol" IEEE Transactions on Security & Privacy Volume: 7 Issue: 1 on pages: 78 – 81
3. Kong, A.W.K.; Zhang, D.; Kamel, M "Analysis of Brute-Force Break-Ins of a Palmprint Authentication System" IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics Volume: 36 Issue: 5 on pages: 1201 – 1205.
4. Coppersmith, D.; Johnson, D. B.; Matyas, S. M "A proposed mode for triple-DES encryption" IEEE Transactions on IBM Jounal of Research and Development Volume: 40 Issue: 2 on pages: 253 – 262.
5. Sung-Ming Yen "Security of a One-Time Password Signature" IEEE Transactions on Electronics Letters Volume: 33 Issue: 8 on pages: 677 – 679 published in 1997.
6. M. Viju Prakash, P. Alwin Infant and S. Jeya Shobana, Eliminating Vulnerable Attacks Using OneTime Password and PassText – Analytical Study of Blended Schema published in 2010.