International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey on One Time Password

Mirza Tanzila Maqsood[1], Pooja Shinde[2]

[1]SRTM University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

[2]SRTM University, Department of CSE, M. S. Bidve Engineering College, Latur, Maharashtra, India

Abstract: ***A password is a sequence of characters used for user authentication to prove identity or access authorization to gain access to the resources which should be kept secret. Passwords are the powerful equipment's that tend to keep all data and information digitally safe. Text based words are most well liked style of user authentication on websites due to its convenience and easiness. The easier the password is for the owner to remember usually means it would be easier for an attacker to guess. And also the security of system can be reduced by passwords that are difficult to remember. However, users' passwords are at risk to be exploited and compromised underneath different threats and vulnerabilities. Security of Password is very important for user authentication on networking system. Passwords are prone to various types of attacks like password stealing attack, password reuse attack, password cracking attack, brute force attack etc. Passwords can be protected by various methods introduced by different researchers. To decrease the harm caused by phishing and other attacks, banks, governments, and other industries are deploying One-Time Password systems. In this paper, we proposed a survey about One-Time Password.***

Keywords: Network security, Password reuse attack**,** Password cracking system, User authentication.

1. Introduction

In networking system, since most of the activities exist on internet and user authentication is the most essential component within the field of Security. Computer users are asked to create, preserve and remind an increasing number of passwords for host accounts, email servers, online financial services and e-commerce sites. Password based user authentication can defend against dictionary attacks and brute force attacks if users opt for strong passwords to provide enough entropy. Most users choose easy to remember passwords (i.e., weak passwords) even if they know that these passwords might be unsafe. Another decisive problem is that users tend to reuse same passwords across a variety of websites. Negative influence of human factors is the basic reason behind all the above problems.

Thus far, researchers have investigated a variety of technologies to trim down the negative influence of human factors in the authentication procedure. Since humans are more skillful in remembering graphical passwords than text passwords, many graphical password strategies were designed to deal with human's password recall problem. Hence, Password management tools were designed. Strong passwords are automatically generated by these tools, which discourses password reuse and password recall problems. Here, users have to memorize a master password to access the password management tool. Three factor authentication is another attractive strategy. It is a method of computer access control in which user is granted access after successfully presenting several pieces of evidence to an authentication mechanism; of following categories: knowledge (something user know); possession (something user have), and inherence (something users are).For authentication procedure, the user must enter a password and input a pass code generated by the token, and scan the biometric features. Two factor authentication is more eye-catching and convenient than three-factor authentication. Two factor authentication is a authentication procedure in which user has to provide two means of identification from different categories; first is a personal token, such as a card, and second is the memorized security code. Disadvantage is that users simply forget to carry the token

One time password (OTP) systems provide a mechanism for logging on to a network or a service using a unique password which can be used only once, as the name suggest. This prevents some forms of identity theft by making sure that captured username/password cannot be used second time. Typically user logon name stays same, and one time password changes with each login. One time passwords are a form of so-called strong authentication, provides much improved protection to on-line banking accounts, corporate networks and other systems containing sensitive data. Strong authentication systems addresses the limitations of static passwords by incorporating an additional security credential, a one-time password (OTP) strategy, to protect network access and end users digital identities. This adds an extra level of security and it will be extremely challenging for an attacker to access unauthorized data, networks or online accounts.

2. Related Work

2.1 Methods of generating OTP

OTP generation algorithms make use of pseurandomness or randomness, and also hash functions, which can be used to obtain a value but are hard to reverse and therefore hard for an attacker to obtain the records used for hash.

2.1.1 Time Synchronized

A time synchronized OTP is generally related to a piece of hardware called a security token (one time password is generated by this token).Inside the token, there is an accurate clock which is synchronized with the clock on the authentication server. Time based One Time Password Algorithm (TOTP) is an example of time synchronized OTP of standard .TOTP is an algorithm that calculates one time password from a shared secret key and the synchronized

current time. TOTP is an example of an hash based message authentication code (HMAC).By using a cryptographic hash function, the shared secret key is combined with the current timestamp and one time password is generated.

2.1.2 Mathematical Algorithm

A mathematical algorithm generates a new password based on the previous passwords (OTPs are efficiently a chain that must be used in predefined order).Here, new password is based on a challenge (a random number chosen by the authentication server or transaction details) and/or a counter. Each new OTP is created from past used OTPs.

2.2 Methods for delivering OTP

2.2.1 Text Messaging

A frequent technology used for the delivery of OTPs is text messaging. Because text messaging is an ever-present communication channel, and is directly available in almost all mobile handsets and, through text-to-speech conversion, to any landline telephone or mobile handset, text messaging is likely to reach all customers with a low cost to implement. OTP over text messaging might be encrypted using an A5/x standard, which some hacking groups report can be effectively decrypted within minutes or seconds, or the OTP over SMS might not be encrypted by one's service-provider at all[13]. The mobile phone operator becomes a part of the trust chain. In the case of roaming, more than one mobile phone operator has to be trusted. Using this data may increase a man-in-the-middle attack

2.2.2 Mobile phones

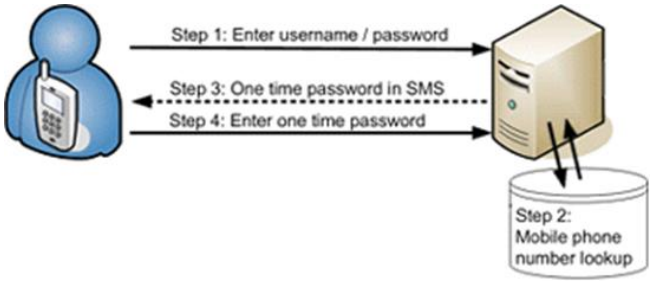

Figure 1: Steps to get OTP on Mobile Phone

A mobile phone keeps costs low as a very large number of people use mobile phone for various reasons other than generating OTPs. Mobile phones additionally support any number of tokens within one installation of the application [13], and from one device user will be authenticated to multiple resources. Model-specific applications according to user's mobile phone are also available.

2.2.3 Proprietary tokens

Figure 2: [15] HID Display Card Token

HID Display Card Tokens enable organization to apply strong authentication to their network, system and cloud based applications. The Display Card tokens fit easily into user's wallet, and are highly portable and convenient .When needed, users simply click a button and Display Card Token generally generates a one-time password they can use to authenticate to the resource they need[15].

Figure 3: [13] RSA Secure ID Token

RSA SecureID is an alternate type of token which is used for generating one time passwords. More advanced hardware tokens use smart cards that are microprocessor based to calculate one time passwords. Smart cards are used for strong authentication and include data storage capacity, processing power, portability and ease of use. They are fundamentally more secure than other OTP tokens because they store personal data, and do not transmit personal or private data over network.

2.2.4 Web based methods

Authentication offers various web based methods for delivering one time passwords without the use of hardware tokens. Such techniques depend on user's ability to recognize pre-chosen categories from a randomly generated collection of pictures. When registering on a website, the user chooses several categories of pictures; such as animals, cars, celebrities and flowers. Whenever user would login the website they are presented with a randomly generated grid of picalphanumeric character overlaid on it [13]. The user looks for pictures that fit their pre-chosen categories and enters the associated alphanumeric characters [13] to form one time password.

2.2.5 Hardcopy

In some countries for online banking, the bank sends user a list of OTPs that are printed on paper. Other banks send plastic cards with actual OTPs covered by a layer that the user has to scratch off to disclose a numbered OTP. To carry out online transaction, the user is required to enter a specific OTP from that list. Some system inquire for numbered OTPs sequentially, others pseurandomly choose an OTP to be entered.

3. Work Done

In [1], M.Wu, S. Garfinkel, and R. Miller, proposed an authentication protocol which uses a mobile phone as a hand-held authentication token, and a security proxy which allows the system to be used with unmodified third-party web services.In [3], J. A. Halderman, B. Waters, and E. W. Felten have proposed a technique that uses strengthened cryptographic hash function to compute secure passwords for arbitrarily many accounts while requiring the user to memorize only a single short password. In [4], B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell have describe a browser extension, PwdHash that strengthens web password authentication and transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks. Since the browser extension applies a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and (optionally) a private salt stored on the client machine In [5], K.-P. Yee and K. Sitaker have described a tool named Passpet which improves both the convenience and security of website logins through a combination of techniques. Passpet uses password hashing that helps users to manage multiple accounts by turning a single memorized password into a different password for each account. In [7], B. Parno, C. Kuo, and A. Perrig, have proposed a mutual authentication system named Phoolproof, prevention against phishing attack. Phoolproof will create a bookmark on users cell phone and on one click of the bookmark user will be directed to official website. In [8], J.McCune, A. Perrig, and M. Reiter, proposed a protocol named Bump In Ether. In this protocol, User input traverses a trusted tunnel from the input device to the application .The mobile device verifies the integrity of the host platform and application provides a trusted display through which the user selects the application to which her inputs should be directed, and encrypts those inputs so that only the expected application can decrypt them.

In [10], M. Mannan and P. van Oorschot, proposed a MP-Auth protocol (Mobile Password Authentication).In this protocol long term password is entered through personal device such as cell phone. The personal device provides a user's long-term secrets to a client PC only after encrypting the secrets using a pre-installed, "correct" public key of a remote service (the intended recipient of the secrets). The proposed protocol (MP-Auth) is intended to safeguard passwords from key loggers, other malware (including root kits), and phishing attacks.

4. Conclusion

Authentication mechanisms provide the keystone for security of many distributed systems, especially for increasingly admired online applications. For decades, passwords and PINs were used for conventional authentication but now they are insufficient to protect online users and organizations from ever more sophisticated attacks. Number of researchers has studied a variety of methods for security of data on a network, by introducing different one time password security methods. They also gave a diverse experimental results which shows that how these systems are efficient to protect passwords. This study projected about improvement to various traditional authentication mechanisms. The solution introduced here includes a one-time-password (OTP) and incorporates the concept of various levels and various channels. Therefore this paper proposed about to secure user identity and user authentication. Round Robin DNS can be used to enhance the performance of Opass and will also give immediate response from the server for multiple users at a time. In order to perform synchronous conferencing of SMS service web relay chat protocol can be used. In that way communication overhead can be reduced because of many transactions.

References

[1] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy and Security Software, 2004.
[2] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Communication XXXXVII(4), pp. 75–78, 2004.
[3] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," In Proceedings of the 14th International Conference on World Wide Web,pp. 471–479,2005.
[4] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," In Proceedings of the 14th Conference Usenix,Security pp. 2–2, 2005.
[5] K.-P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection," In Proceedings of the second Symposium on Usable Privacy Security, pp. 32–43, 2006.
[6] S. Gaw and E. W. Felten, "Password management strategies for online accounts," In Proceedings of the second Symposium on Usable Privacy and Security, pp. 44–55,2006.
[7] B. Parno, "Phoolproof phishing prevention ," in Financial Cryptography and Data Security, C. Kuo, and A. Perrig, springer-Berlin Heidelberg, New York,2006.
[8] J.McCune, A. Perrig, and M. Reiter, "Bump in the ether: A framework for securing sensitive user input," In USENIX Annual Technical Conference,pp. 185–198,2006.
[9] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser: Analysis of web-based malware",In Proceedings of the first Conference on Workshop on Hot Topics in Understanding Botnets,pp.4-4,2007.
[10] M. Mannan "Using a personal device to strengthen password authentication from an untrusted computer," in Financial Cryptography Data Security, P. van Oorschot, springer-Berlin Heidelberg, New York,2007.
[11] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X.Zhang, "Trustworthy and personalized computing on public kiosks, "In Proceedings of the sixth International Conference, pp.199–210, 2008.
[12] C. Yue and H. Wang, "Session Magnifier: A simple approach to secure and convenient kiosk browsing," In Proceedings of the eleventh International Conference

Ubiquitous Computing, pp. 125–134, 2009.
[13] "One-time password-Wikipedia, the free encyclopedia," [Online]: Available: https://en.m.wikipedia.org/wiki/One-time_password.[Accessed:Feb.12,2016].
[14] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin (2012), "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", IEEE transactions on information forensics and security, pp. 651-663, 2012.
[15] ActiveID DisplayCard Tokens-HID Global [Online]:Available: http://www.hidglobal.com/products/cards-and-credentials/activid/displaycard-tokens.[Accessed:Feb.13, 2016].

Author Profile

Mirza Tanzila Maqsood has received B.E degree in Computer Engineering from Amrutvahini College of Engineering, Sangamner, Pune University in 2009.Now she is pursuing Masters in Engineering(Computer Science and Engineering) from M.S.Bidve Engineering College, Latur, SRTM University Nanded, Maharashtra.

Miss Pooja Shinde has received B.E degree in computer science and engineering from M.S Bidve Engineering college, Latur, SRTM University in 2010.Also she has received M.E degree in Computer Networking and Engineering from Dr.Babasaheb Ambedkar Marathwada University ,Aurangabad in 2014.And now she is working as an Assistant Professor in M.S Bidve Engineering College,Latur.