International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (145-148), Impact Factor: 1.252, Available online at: www.erpublications.com

A Survey: Novel Approach Secure Authentication Technique by One Time Password using Mobile SMS

Preeti Ahlawat[1], Rainu Nandal[2]*
[1,2]University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India

ABSTRACT: In this paper we consider the potential of SMS- one time password (OTP) in results upgradation to get rid of around kinds of hacking methods like phishing and brute force, man in the middle, key-loggers and mostly social engineering and the principle goal of the project is to create a second layer of security to protect the users from those threads by simply require an extra security code that offer from the server to their mobile phone and proposes one-time password mechanism that has enhanced security using public key infrastructure to prevent integrity problems due to birthday attack and hash collision problem occurring from hash function and seamless integration with Active Directory and Web server is achieved. This scheme can work with any verification scheme used with real life to enhance the security and trust factor for the users. This scheme can be used for voters while casting their votes. These techniques provide a more secure platform thus, overcoming vulnerabilities of the traditional voting system.

Keywords: SMS, OTP, Two Way Authority, Trust Factor, Attackers, PAKE (Password Authentication Key Exchange).

1. INTRODUCTION

The deployments of one-time passwords have not used them in the strongest way possible. In a typical usage, Alice visits a bank's website in her browser, views a challenge on the website indicating which one-time password to use, and enters that one-time password into her browser, which transmits the one time password to the website you need to fill in an extra code that sent through text message to your mobile. If you do not want to meet this challenge in the near future logins, you have to save the device to your account since you have given the received security code. As more people change to online services to share and connect with others, any unauthorized access will be taken in order to take more control over protecting their account is what they are looking for. Verifying the attempted account access will be noticed upon the next login session if by any chance we have encountered with. Amongst the whole services provided by supplier center in mobile network, SMS plays an important role with more than 60% used by mobile users in total services in network infrastructure; however, service's price is cheap comparing to other services. [3] SMS stands for Short Message Service.

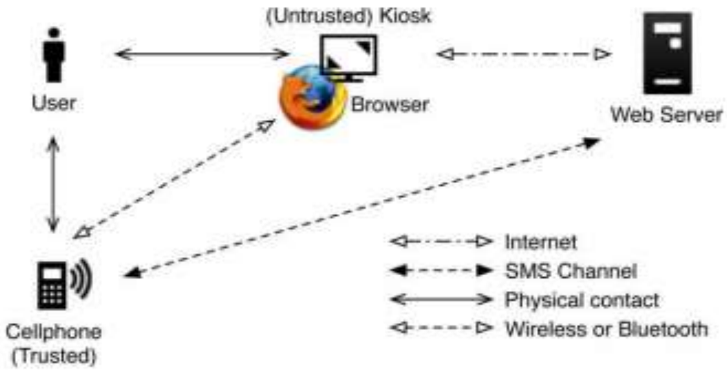

Figure 1: SMS Channel by OTP

SMS One-time Password is a password which provides the authentication to online identity customers. Whenever the customers transact a specific transaction online, they will be provided a SMS notification into their designated cell phone, which is SMS one-time-password coming along with the transaction details and corporate virtual private networks (VPNs) to reduce the damage of passwords compromised through phishing and some spyware attacks. To date, however, they have not been formally studied using techniques from provable security; one existing work [3] presents a PAKE protocol that uses pseudorandom passwords, but does not consider how the security properties of one-time passwords or pseudorandom passwords differ from normal long-term passwords. Provide similar features from other websites requirement.

2. OTP (One Time Password)

A one-time password (OTP) is a password that able to security enhancement and get purely identify valid user. This OTP is based on the very popular algorithm HMAC SHA. The HMAC SHA is an algorithm generally used to perform authentication by challenge response. It is not an encryption algorithm but a hashing algorithm that transforms a set of bytes to another set of bytes.

This algorithm is not reversible which means that you cannot use the result to go back to the source. A HMAC SHA uses a key to transform an input array of bytes. The key is the secret that must never be accessible to a hacker and the input is the challenge. This means that OTP is a challenge response authentication. The secret key must be 20 bytes at least; the challenge is usually a counter of 8 bytes which leaves quite some time before the value is exhausted and requires the one-time passwords be of a particular form (namely, a hash chain), and that future passwords not be revealed then captured old OTP will be no longer valid when you have used it already to log into your account or make a transaction so potential hackers cannot abuse it. Because OTPs are difficult for most of people to memorize so they require more advance technology to get this done. The pseudo randomness is used typically in order to make the usage of OTP generation algorithms.

3. Security Model of one-time-password protocol

The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates. Authentication is based on knowledge of the shared password. Informally, a protocol will provide secure mutual authentication if no honest party Aˆ accepts a session as being with party Bˆ unless Bˆ participated in the protocol, and vice versa. We want a one-time-password protocol to give secure mutual authentication for the current session even if other one-time passwords have been revealed. On the contrary after reading this you should understand why using an OTP as a second factor authentication is extremely secure.

The OTP is very secure for at least the 2 following reasons such as you can’t go back again if you put wrong entity in a single session, and in other hand we can’t go back again to source until session will not go for initial page because session would be expire until execute the query page for OTP generator page. And restriction can be achieved by having each party maintain a record of used one-time passwords.

4. Related Work

The protocol is a message-driven protocol One-time passwords are also being used for stronger authentication in virtual economies such as World of Warcraft [Bli09]. The Internet Engineering Task Force (IETF) has standardized various mechanisms for deriving [1,3] and using [4,1] one-time passwords. While all of these systems may generate and deploy one-time passwords securely, none of them proceed to use one-time passwords in cryptographically secure way. Password-authenticated key exchange was first introduced by Bellovin and Merritt in 1992 [4] as a protocol in which the client and server share a plaintext password and exchange encrypted information to allow them to derive a shared session key. A later variant [BM93], often called verifier-based, removed the requirement that the server have the plaintext password, instead having a one-way transformation of the password.

The most extensively used model for the security of PAKE protocols is the Bellare-Pointcheval-Rogaway (BPR) model [1] and its extension [5] for verifier-based protocols. This model is the starting point of our model for the security of one-time-PAKE protocols. Koot [6] provides a simple risk analysis of mTAN security for iOS as well as Android smartphones. The work fails to provide an in-depth study of the root causes of mTAN insecurity. They do not aim to secure mTAN, but rather try to link the mobile phone to the computer used for online banking. Several studies conducted on mobile malware [2,7] show that authentication credential stealing mobile malware exists in the wild. In this work, we present countermeasures that specifically protect against mobile malware that is built to intercept and exfiltrate authentication credentials sent via SMS.

A large scale study [6] evaluated authentication schemes in general using three main characteristics: usability, deployability, and security. Characteristics basically attest SMS OTP with maximum points besides two issues. These issues are: not Resilient-to-Internal-Observation and not Resilient to-Theft. Our virtual dedicated channel makes SMS OTPs Resilient-to-Internal Observation and thus increases the security of SMS OTP significantly.

An observer (attacker) easily eliminates non-GridPasse character introduce Bell and Gatt in 1999 [7] by observing GridCodee digits over time. This weakness cannot be totally eliminated. In most cases, the weakness can be improved by utilizing pre-installed software that shuffles GridCodee digits in the sequence only known by the client side and the authentication server side before transferring the digits over the network. However, it is not free from over-the-shoulder or key logging attacks, because the order of the GridCodee is exposed with over-the-shoulder and key logging attacks.

5. Discussion

The original product can worked on implemented one of the first versions of the OTP in a Javacard was using an OTP token with a screen or a mobile phone with a card applet to generate the OTP. In this model both the server and the authentication token have to generate an OTP that must be synchronized. The process is the following: The user generates an OTP with his token, type it and press OK. The server receives the OTP generated by the token, it increments the counter and generates a new OTP. This is where there is a possible synchronization issue.

Synchronization issues in Accessing:

If the user enters the correct OTP, then the server when it increments the counter and calculate the OTP, the authentication will be successful. Now there could be few scenarios that could lead to a de-synchronization of the server counter and the authentication mechanism won't work. In some cases it could be possible to resynchronize automatically the counter but in some cases the user would have to resynchronize the server counter using a specific procedure. When people are being hacked, most of them are complaining about some virus from their computer which can steal their password but actually it comes from their unconscious actions on the network.

Some Structure of de-synchronization could occur:

1. The user accidentally press the generate button of his token and doesn't perform an authentication. In this case the counter of the token would be ahead of the server counter by few steps.
2. The user enters an OTP without generating it from the token. In this case the counter of the server would be ahead of the token counter.
3. The user generates an OTP with the token but types a wrong OTP.

If the OTP given by the server can try to auto-resynchronize itself by trying few counters around the expected counter. In our server we would use 10 values around the nominal counter value. If the synchronization cannot be done, the server would retain the current counter value in order not desynchronize the server further. However the server would have to implement a strategy to inform that the server and token are totally desynchronized and a manual synchronization must be performed.

Physical synchronization process:

The server can propose a manual synchronization process to the user. The OTP numbers are only 8 digits generated by the hash of 8 bytes counter and formatting a 20 bytes result. This means that it is possible to get twice the same OTP for 2 different counter values. So attempting synchronization with only one OTP value is not reliable. A manual resynchronization process needs the user to enter 2 consecutive OTP, and then the server can try to find the requested sequence as the probability to get the same sequence of 2 OTPs for different counter values is extremely low if not zero.

6. Conclusion

The cryptographic countermeasures are bypassed. For any PAKE protocol to succeed, user training and user interface design will be very important. Spyware remains a significant threat to password security. In the face of passive spyware, such as a keystroke logger which collects information and occasionally relays it back to the attacker and 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. For future study we can provides a better security as it ensures that no voter is allowed to vote more than once. Also the system takes care that no voter can determine for whom anyone else voted and no voter can duplicate anyone else's vote. Every voter can make sure his/her vote is cast.

References

[1]. SMS introduction [online]. ActiveXperts software; 2013URL: http://www.activexperts.com/xmstoolkit/sms/intro/ Accessed 3 March 2013.

[2]. Benefits of SMS. VISUALtron; 2013 URL: http://www.visualgsm.com/wire_sms_topic02.htm Accessed 3 March 2013.

[3]. One-time password [online]; March 2013 URL: http://en.wikipedia.org/wiki/One-time_password Accessed 3 March 2013.

[4]. The S/KEY One-Time Password System [online]; March 2013 URL: http://tools.ietf.org/html/rfc1760 Accessed 3 March 2013

[5]. 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

[6]. M. Abadi, L. Bharat, and A. Marais, "System and method for generating [3] unique passwords," U.S. Patent 6 141 760, 1997.

[7]. Eun-Jeong Choi, Chan-Oe Kim, JooSeok Song, "Password-Based Authentication Protocol for Remote Access using Public Key Cryptography", KIIS Journal, VOL. 30 NO. 01, 2003.02, pp. 0075˜ 0081.

[8]. SKINNER, C. "75% of young adults want to vote by sms in the election. 89% expect text voting to be introduced soon". PC ADVISOR. February18, 2010.