Enhanced Multi-factor Out-of-Band Authentication En Route to Securing SMS-based OTP

Ariel Roy L. Reyes¹*, Enrique D. Festijo², Ruji P. Medina¹

¹Graduate Programs, Technological Institute of Philippines, Quezon City, Philippines
²Technological Institute of the Philippines, Manila, Philippines

Received 24 October 2018; received in revised form 17 November 2018; accepted 13 December 2018

Abstract

Validation of user’s authenticity through authentication played a crucial role to address risks and security issues in today’s connected world. Among different authentication methods, OTP sent via SMS was identified as the most commonly used multi-factor authentication mechanism. However, studies have shown that it has not remained attack-proof. It has been branded to be vulnerable to SMiShing, a technique comparable to Internet phishing, and Eavesdropping accomplished through keylogging, screens capturing, shoulder surfing and other social engineering practices. This study introduced an innovative approach to secure SMS-based OTP against its threats through OTP encryption using modified Blowfish algorithm. A mobile application was also employed for capturing and processing encrypted SMS-based OTP to produce new OTP for verification, thus performing end-to-end OTP. Experimentation results and analysis revealed that the proposed architecture was free against the said vulnerabilities and promote tighter security, making it a good alternative for SMS-based OTP multi-factor authentication.

Keywords: Blowfish-128, eavesdropping, SMiShing, SMS-based OTP

References


* Corresponding author. E-mail address: copperstone1999@gmail.com
Tel.: +639198763561


[21] CrackStation - online password hash cracking - MD5, SHA1, Linux, rainbow tables, etc. Available: https://crackstation.net/

Copyright© by the authors. Licensee TAETI, Taiwan. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license (https://creativecommons.org/licenses/by-nc/4.0/).