

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

Ariel Roy L. Reyes^{1*}, 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

- [1] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for the multi-server environment using ECC," *Computer Communications*, vol. 110, pp. 26-34, 2017.
- [2] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Computers & Security*, vol. 63, pp. 85-116, 2016.
- [3] M. H. Barkadehi, M. Nilashi, O. Ibrahim, F. A. Zakeri, and S. Samad, "Authentication systems: a literature review and classification," *Telematics and Informatics*, vol. 35, pp. 1491-1511, 2018.
- [4] M. Belk, C. Fidas, P. Germanakos, and G. Samaras, "The interplay between humans, technology and user authentication: a cognitive processing perspective," *Computers in Human Behavior*, vol. 76, pp. 184-200, 2017.
- [5] J.-J. Huang, W.-S. Juang, C.-I. Fan, Y.-F. Tseng, and H. Kikuchi, "Lightweight authentication scheme with dynamic group members in IoT environments," in *13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services*, New York, NY, USA, 2016, pp. 88-93.
- [6] M. Gerami and S. Ghiasvand, "One-time passwords via SMS," *Bulletin de la Société Royale des Sciences de Liège*, vol. 85, pp. 106-113, 2016.
- [7] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, "Mind your SMSes: mitigating social engineering in second-factor authentication," *Computers & Security*, vol. 65, pp. 14-28, 2017.
- [8] A. R. L. Reyes, E. D. Festijo, and R. P. Medina, "Securing one time password (OTP) for multi-factor out-of-band authentication through a 128-bit blowfish algorithm," *International Journal of Communication Networks and Information Security*, vol. 10, pp. 242-247, 2018.

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

Tel.: +639198763561

- [9] Y. Yu, J. He, N. Zhu, F. Cai, and M. S. Pathan, "A new method for identity authentication using mobile terminals," *Procedia Computer Science*, vol. 131, pp. 771-778, 2018.
- [10] M. Balduzzi, P. Gupta, L. Gu, D. Gao, and M. Ahamad, "MobiPot: understanding mobile telephony threats with honey cards," in *11th ACM on Asia Conference on Computer and Communications Security*, New York, NY, USA, 2016, pp. 723-734.
- [11] E. Sedyono, K. I. Santoso, and Suhartono, "Secure login by using one-time password authentication based on MD5 hash encrypted SMS," in *International Conference on Advances in Computing, Communications and Informatics*, Mysore, India, 2013, pp. 1604-1608.
- [12] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: a systematic literature review," *Information and Software Technology*, vol. 94, pp. 30-37, 2018.
- [13] C. Shen, Y. Chen, and X. Guan, "Performance evaluation of implicit smartphones authentication via sensor-behavior analysis," *Information Sciences*, vol. 430-431, pp. 538-553, 2018.
- [14] A. S. Chaudhari, "Security analysis of SMS and related technologies," in *Master's Thesis*, Department of Mathematics and Computer Science, Eindhoven University of Technology, 2015.
- [15] D. Yadav, D. Malwe, K. S. Rao, P. Kumari, P. Yadav, and P. Deshmukh, "Intensify the security of one time password using elliptic curve cryptography with fingerprint for e-commerce application," *International Journal of Engineering Science and Computing*, vol. 7, pp. 5480-5482, 2017.
- [16] D. Zhao and W. Luo, "One-time password authentication scheme based on the negative database," *International Journal of Engineering Science and Computing*, vol. 7, pp. 5480-5482, 2017.
- [17] A. R. L. Reyes, E. D. Festijo, and R. P. Medina, "Blowfish-128: a modified blowfish algorithm that supports 128-bit block size," in *8th International Workshop on Computer Science and Engineering*, Bangkok, Thailand, 2018, pp. 578-584.
- [18] S. E. S. Taba, I. Keivanloo, Y. Zou, and S. Wang, "An exploratory study on the usage of common interface elements in android applications," *Journal of Systems and Software*, vol. 131, pp. 491-504, 2017.
- [19] L. Wei, Y. Liu, and S.-C. Cheung, "Taming android fragmentation: characterizing and detecting compatibility issues for android apps," in *31st IEEE/ACM International Conference on Automated Software Engineering*, Singapore, Singapore, 2016, pp. 226-237.
- [20] Password checker online. Available: <http://password-checker.online-domain-tools.com>
- [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/>).