International Journal of Engineering and Technology Innovation, vol. 9, no. 2, 2019, pp. 145-154

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

Ariel Roy L. Reyes[1*], Enrique D. Festijo[2], Ruji P. Medina[1]

[1]Graduate Programs, Technological Institute of Philippines, Quezon City, Philippines

[2]Technological 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

1. Introduction

Advancement in technology triggered users to rely on carrying out various activities through online services that offer accessibility and convenience. Unfortunately, most of these services work on an unsafe channel that brings risks and security issues, one of the most important concern in today's connected world [1-2]. Therefore, a robust security requirement for the online environment is necessary to obtain the trust and confidence of every user.

To better enforce security in online services, authentication has been the major means of defense [2]. It was considered as the primary line of protection that plays a crucial role to verify and validate the authenticity of a user before gaining access to protected systems or allowing online transactions [3]. Various authentication schemes classified as either knowledge-based, token-based, and biometric-based emerged. These schemes use different factors to warrant the authenticity of users that includes anything the user know for Knowledge-based, user possession for Token-based, and user's features for Biometric-based. A combination of these schemes is the latest evolving developments were password combined with PIN code and One Time Password (OTP) as the most widely used authentication method in a two-factor or multi-factor authentication [3-4]. OTP provides an additional layer of authentication that augments username and password [5]. It has been projected to continuously prevail in the coming years because of ease of use, implementation speed, cost-effectiveness, security, and privacy protection [4]. To this end, Short Message Service (SMS)-based One Time Password (OTP) remains one of the most commonly used multi-factor authentication and authorization mechanism that has found wide use such as in online banking,

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

email services, social networks, transactions with financial institutions, online marketplaces, and online academic information applications [6-7]. SMS-based OTP is a method of sending a plaintext code known as OTP through SMS that is valid only for one session or transaction and is expected to expire at a certain time. This scheme effectively reduced risks against illegitimate access [6]. However, this enhanced system has not remained attack-proof [8-9]. SMS Phishing or SMiShing, and Eavesdropping were amongst the identified vulnerabilities of SMS-based OTP as illustrated in Fig. 1.

Fig. 1 SMS Vulnerabilities

SMiShing is a technique comparable to Internet phishing where users are tricked to use their credentials and verification codes on the fake login page with the help of social engineering practices, and a possible malware installed on the user's mobile phone. Eavesdropping, in contrast, is to secretly acquire relevant information such as the verification code through Key Logger, Screen Capturing, and Shoulder surfing [7]. Research revealed 50% and 25% success rate of a social engineering attack against Google's SMS-based authentication and with an out-of-band authentication modality respectively. An increase in the number of attacks using this method has been observed and reported, with twenty-two (22) instances of such attack in China in a so-called Verification Code Forwarding Attack or VCFA [10]. Therefore, a need for a vigorous and safer SMS-based OTP modality in the online world is justified.

This paper aimed to introduce an alternative authentication modality to secure SMS-based OTP using a modified Blowfish algorithm, hereafter refer as Blowfish-128, and an end-to-end OTP for real-time authentication. Blowfish-128 was designed to capitalize on the strengths of Blowfish algorithm while escalating its input text support to 128-bits block size [8]. The primary focus of this paper is to ensure the confidentiality of an SMS-based OTP by (1) Eradication of SMiShing through OTP protection and mobile application transaction confirmation, (2) Elimination of Key Logging, Screen Capturing, Shoulder surfing and related attacks by way of escaping on manual entry of text-based verification code via physical or onscreen keyboards, and (3) Strengthen OTP security as a result of Blowfish-128 OTP encryption and end-to-end OTP implementation through encapsulation of additional information known only between Web and mobile applications, and the users. This study will be a good contribution to the continuous developments in the field of information security and will be a good alternative approach to secure OTP for multi-factor out-of-band authentication implementations.

2. Literature Review

2.1 One time password (OTP)

OTP was first suggested by Leslie Lamport in the early 1880s, and thereafter, many OTP tokens emerged and even patented [5]. It is a technology used to counter attacks against traditional method of authentication, which is with the use of a username and a password. It supplements the use of username and password to enhance security on protected systems. From its

name, One Time, it is actually a code or a password that is valid only for a single session or transaction. This means that for a possible intrusion of OTP that was already used in a transaction, intruders could not exploit anymore and use it to other transactions as it will no longer be valid [11].

Typically, there are three approaches to how OTPs are generated. The first method is through time-synchronization between a server and a client where OTPs generated in this manner are usually applicable, only for a short period of time. The second approach is a mathematical algorithm where the generation of new code is dependent on the previously generated code. Using a mathematical algorithm based on a challenge or a counter to generate a new code is the third strategy [6]. Several models were introduced for the implementation of OTP. It can be either in a paper, web-based application or via an out-of-band modality such as the SMS. Among these models, the most commonly implemented method is sending OTP through an out-of-band medium or through SMS.

2.2. Authentication and OTP

Security and privacy of user's information are important issues in an online environment where authentication plays a crucial role. It verifies the authenticity of a person's identity trying to access a protected system to ensure that an unauthorized retrieval of confidential information is prevented [1, 3]. There are various techniques employed to perform authentication classified as knowledge-based, token-based, and biometric-based authentication schemes. Knowledge-based uses knowledge factors associated with what the user knows such as text and graphical passwords. Whereas, Token-based refers to the use of what users own or is dependent on possession factors like smartphones and the like. The biometric-based scheme, on the other hand, is dependent on inherence factors or factors identifying users like facial features, fingerprints or other biometrics [4, 12]. Each of these models has its own strengths and weaknesses and are subject to different threats and drawbacks [3].

To enhance security and provide stronger authentication, these techniques are combined and is called multi-factor authentication. It may be a combination of Knowledge-based and Token-based, Knowledge-based and Biometric-based, Token-based and Biometric-based, or even a combination of all models [12]. Knowledge-based particularly the use of passwords combined with other possession factors such as OTP and Pin code remains the most used authentication scheme today [13] and perceived to continuously prevail in the coming years because it can be easily and inexpensively implemented while ensuring security and privacy [4]. A very good example of the combination of different factors is the SMS-based OTP for multi-factor out-of-bound authentication.

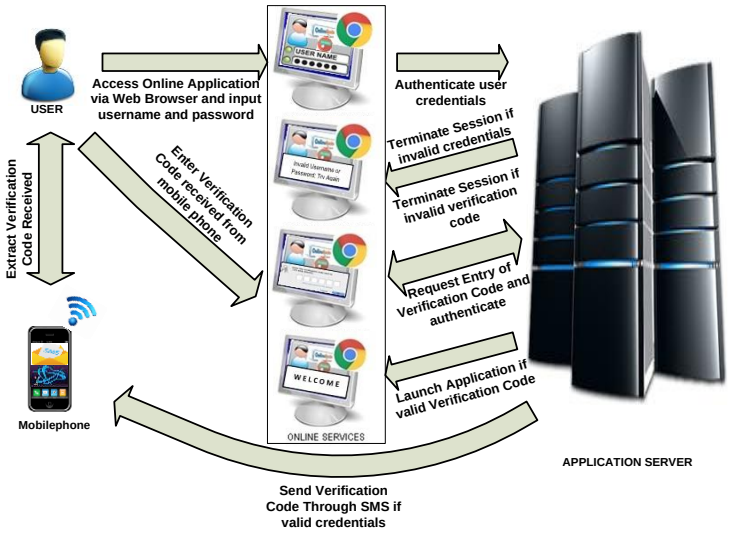


Fig. 2 SMS-based OTP Operation

SMS-based OTP is widely used for multi-factor authentication and authorization scheme of many different applications because all it requires is a mobile phone as an additional device. In an SMS-based OTP system (Fig. 2), users were required to

provide something they knew (username, and password) and something they have (OTP verification code) before access to the secured system is granted. Thus, effectively reducing risks against illegitimate access since both factors have to be broken or to be compromised [6].

As shown in Fig. 2, SMS-based OTP starts with a generated verification code sent via SMS to a registered mobile phone number of a user if the supplied username and password are authentic. The verification code is normally presented as plain text to be readable to users for encoding on online service provider's web application. Access is granted only if encoded verification code matched with that code sent via SMS and before its expiration. Presenting SMS-based OTP in plaintext exposes verification code to various threats and vulnerabilities.

2.3. Vulnerabilities with SMS-based OTP

The vulnerabilities of SMS lies in the messaging service and the available functionalities of mobile networks that became an attractive area for attackers [14]. Phishing has been identified and recorded to be on the rise in many real-world instances. SMS Phishing or SMiShing, is a technique comparable to Internet phishing where users are fooled by a non-genuine message that looks interesting to steal OTP issued by online service providers. This technique is normally accomplished with the help of social engineering practices and possible malware installed on the user's mobile phone [7, 14]. Instances of phishing attacks had been recorded. Citizen Lab recorded events where users were deceived to use their credentials and verification codes on the fake login page. Symantec also revealed cases where users were lured to forward verification codes to an attacker. A new form of phishing, called Verification Code Forwarding Attack (VCFA) was also discovered with a success rate of 25%. VCFA is accomplished by attackers pretending to be the service provider that sends deceiving message for the user to share the verification code [7].

Another common threat is to eavesdrop a verification code. Eavesdropping or to secretly acquire relevant information can be accomplished using Key Logger, Screen Capturing, and Shoulder surfing. Keylogger attack captures all user keystrokes and sends logs periodically to the attacker. Often, with the combination of Keylogger, Screen capturing captures both the keystrokes and visual items. Screen capturing attack can also take the screenshots of the whole screen to retrieve confidential information. Shoulder surfing, on the other hand, is a technique that discloses sensitive information by merely looking at the keyboard or the screen while users perform online transactions [14]. The foregoing threats necessitate the need to hide sensitive information such as OTP verification codes from adversaries.

3. Related Work

To date, various works had been introduced to counter security issues faced by OTP-enabled transactions in the online environment. In [15], the security of OTP transmitted to the user was intensified through Elliptic Curve Cryptography (ECC) and fingerprint biometric for OTP encryption. The OTP, in this model, was encrypted using ECC with biometric before transmission to user's mobile. The same method was also introduced in [6], OTP was protected during transmission but with the involvement of highly complex non-return encryption algorithm. In the same manner, both models decrypt OTP at user's mobile to produce plaintext OTP for input in service provider's panel. These models intensified protection of OTP during transmission on an untrusted channel; however, vulnerabilities that include VCFA, Eavesdropping and other related treats associated with plaintext OTP input on service provider's web service or panel are welcomed. An OTP authentication scheme based on the negative database was also introduced in [16]. In this enhanced authentication system, the most essential information is password and the random seed that should be generated and shared with the server. This requires a secure channel and mutual authentication scheme to provide server spoofing immunity. These developments simply require a better solution at lower implementation cost to provide safer OTP-based authentication system or enhance OTP protection not only during transmission on unsafe medium but even until successful authentication.

4. System Architecture

The proposed system architecture has two components: the Web-Based Application (WBA) and the End-User Application (EUA), as shown in Fig. 3. Both components work seamlessly to strengthen security against the identified vulnerabilities of SMS-based OTP on authentication systems.

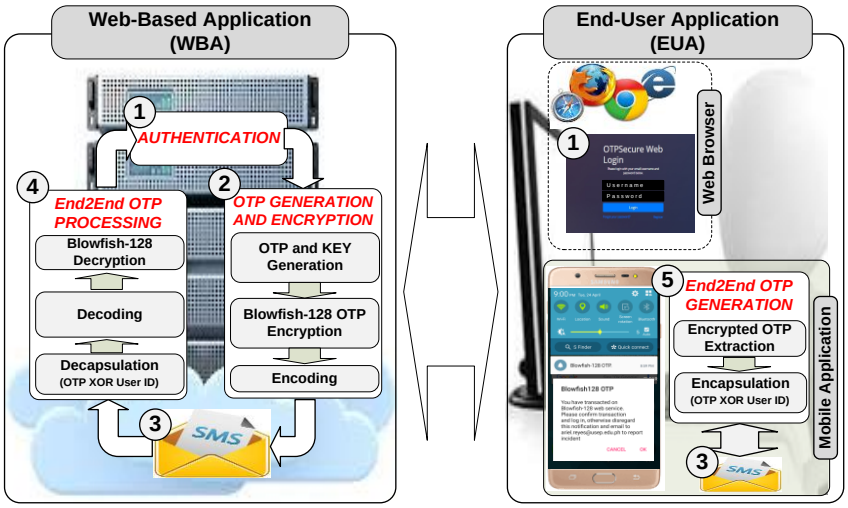


Fig. 3 Proposed System Architecture

4.1. Web-based application (WBA)

In the WBA, authentication with the use of username and password served as its starting point, just like any other Knowledge-based authentication models (Fig. 3-①). Authentic username and password are required to acquire verification code through user's registered mobile number via SMS (Fig. 3-③), otherwise, access to WBA is not permitted. Given an authentic credential, OTP Generation and Encryption of the WBA perform generation of OTP and Secret Key, encryption of OTP using Blowfish-128, and encoding of the encrypted OTP with base64 (Fig. 3-②). Blowfish-128 was the first version of Blowfish algorithm modification designed to support 128-bits block size while capitalizing on the strengths of the Blowfish algorithm. It implements a dynamic selection encryption method and reduction of the execution of cipher function in randomly determined rounds that improved the algorithm's performance, security, complexity and the execution time [8, 17]. The output of the OTP Generation and Encryption will be the encrypted verification code/OTP to be transmitted to the user's registered mobile number via SMS (Fig. 3-③). It was designed to expire at a specified time. Thus, the user needs to confirm the transaction through EUA before expiration to gain access with the WBA in real time.

After the receipt of the SMS reply from the EUA before the predefined expiration time, End2End OTP Processing commences (Fig. 3-④). End2End OTP Processing performs Decapsulation, Decoding, and Decryption followed by authentication (Fig. 3-①). Decapsulation refers to the removal of the user ID from the received OTP through an XOR operation in order to prepare the OTP for Decoding (Fig. 3-④). In this phase, the received new OTP will be XORed with the registered User ID encoded by the user during account registration. Decoding recovers the original OTP representation after being encoded to base-64. Decryption using Blowfish-128 recuperates the generated verification code/OTP for authentication (Fig. 3-①). If incorrect information is retrieved or OTP has expired, access to WBA is not allowed. Given a successful authentication process that validated registered user's mobile number, user ID, and the verification code/OTP, users gain access to the WBA.

4.2. End-user application (EUA)

The verification code sent by WBA was not displayed on EUA interface to protect against SMiShing or Eavesdropping. Instead, EUA installed on a smartphone capture and process it to notify the user of the transaction made with the WBA. After

the receipt of the verification code/OTP from WBA, user confirmation through the EUA enables the creation of a new OTP through End2End OTP Generation (Fig. 3-⑤). In this phase, received OTP will be extracted from the received verification message and XORed with the User ID. The output served as the new OTP to be sent back as a reply to WBA via SMS (Fig. 3-③), thus, performing end-to-end OTP. After sending the new OTP to the WBA, authentication, and verification is performed by the WBA allowing the user to gain access on it in real time provided all details are valid. This added an additional layer of security known merely between the WBA, EUA and the registered user.

5. Results and Discussions

The proposed architecture was implemented and tested in a Pentium, Dual Core-powered CPU with 4GB of memory and running on Windows 10 64-bit operating system. The WBA component was implemented using XAMPP v3.2.1 to provide a web server solution stack. CodeIgniter v3.1.7, an application development architecture, was also used in the development of the WBA. Sending and receiving of SMS messages to and from a registered user were materialized using Pierpaolo Libanori's HTTP SMS Server, a multi-user SMS gateway software implemented with an HTTP server and is freely available at Google Play.

The EUA was designed for the Android mobile operating system (OS) based smartphones as it was the most popular mobile OS with the highest market share [18-19] and the development platform used was Android Studio. To evaluate the performance of the proposed architecture, a group of ten (10) individuals having a mobile phone with Android OS versions 6 to 8 were asked to experience using the solution in a mini-laboratory setup. Users were first asked to create user accounts by providing relevant information and requested to install EUA on their mobile phone. After accounts were registered, users logged in with WBA and the time consumption (OTP generation and verification time) was recorded for every successful login. The time involved in the transmission of OTP via SMS was not considered as this was beyond the control of the proposed architecture.

5.1. WBA simulation result

As presented in the WBA Process Flow (Fig. 4), user's account was necessary, thus, first-time users were mandated to create an account and supplied relevant information including User ID and mobile number. The user ID was derived from the extracted Android ID displayed on the user's mobile device after EUA installation and was used as one among multiple factors in the verification phase to determine the authenticity of the user along with the registered mobile number and the encrypted OTP. Given an authentic username and password, OTP generation, encryption, and transmission commence where the creation of OTP marked its starting point. Several standards and proposed methods for generating OTP has been used commercially that offered good security, but for the purpose of the conduct of the experiment, OTP in this study was simply generated as a 128-bits random representation that served as an input for Blowfish-128 encryption to make OTP indecipherable to illegitimate users and promote a safer transaction. In [8], Blowfish-128's performance has been measured in terms of avalanche effect, integrity check, and execution time and was observed that at 128-bit input block size, improvement of utmost 5.91% for avalanche effect, 38.97 % for integrity, and 41.03% for execution time were recorded as compared to Blowfish algorithm. Meanwhile, in [17], it was evaluated under varied input lengths in terms of avalanche effect, throughput, and execution time and experimental results showed improved performance and execution time and had increased the degree of complexity and diffusion. After OTP encryption, encoding of the encrypted OTP to base64 representation worked as the final phase before transmission of OTP to the registered mobile number of the user. The average recorded time to complete these processes was 0.163 milliseconds per user making the system responsive to multiple user's requests.

The system waits for user confirmation via EUA (Fig. 4). After the receipt of a reply from EUA that corresponds to the new OTP, Multi-factor extraction that embraces Decapsulation, Decoding, and Decryption through Blowfish-128 processes was performed. Decapsulation refers to the removal of the user ID from the received OTP through XOR operation. Conversion

from base64 to hexadecimal representation followed before decryption. Real-time Multi-Factor Authentication embarked after extraction of multiple factors that guaranteed the legitimacy of the user by comparison of the extracted details from received OTP including the mobile phone number, the extracted user ID, and the verification code/OTP against what was stored in WBA's database. A match granted user access (Fig. 4(h)), otherwise, access was not allowed (Fig. 4(g)). The entire process consumed an average of 0.915 milliseconds, a good result allowing its use for application with multiple users. On the other hand, for too long confirmation that reached expiration, the user was informed that the verification code/OTP has expired (Fig. 4(g)). An anti-brute force mechanism was also implemented in WBA by locking the system after a series of multiple failed login attempts which is similar to Google's Gmail user authentication scheme.

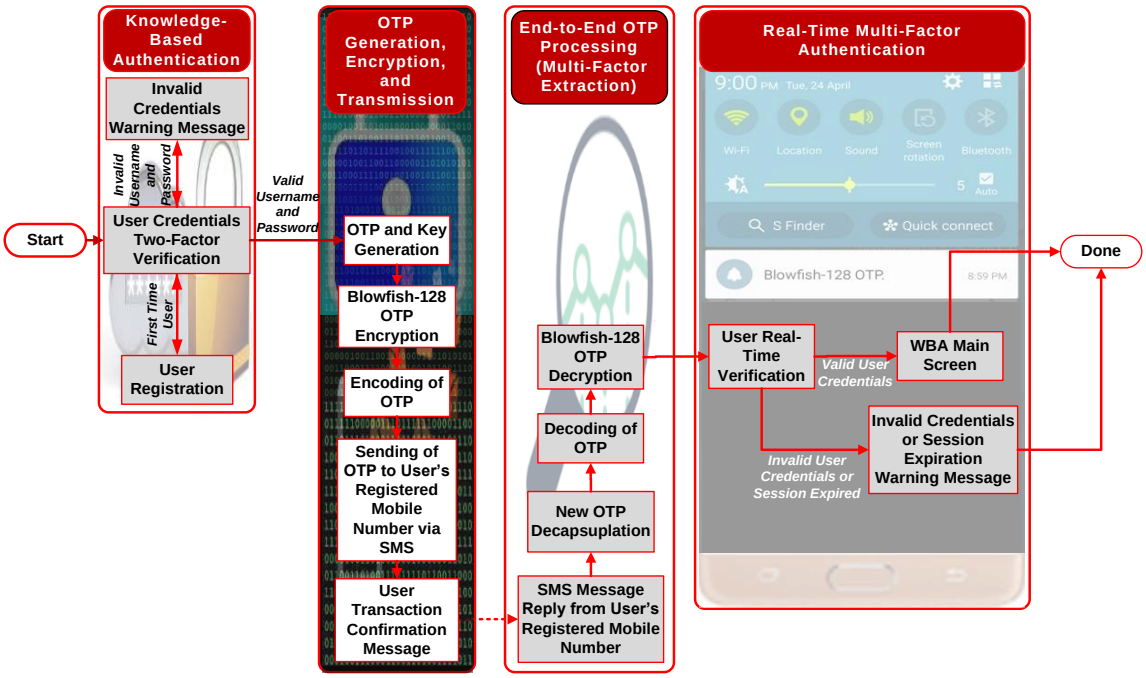


Fig. 4 WBA Process Flow

To further test the security strength of OTP to be transmitted via SMS to EUA, an assumption of its illegitimate acquisition by adversaries was considered. Generated OTP of the proposed architecture was subjected to online password cracker by Online Domain Tools to determine brute-force attack cracking estimated time and dictionary attack check [20]. It was also subjected to Crypto Bench and Crack Station, the commonly used cryptanalysis tool identified by Infosec Institute [21] and a free online password hash cracker respectively. Presented in Table 1 is the comparison of brute-force cracking estimated time and dictionary attack check between the proposed architecture's generated OTP and plaintext OTP.

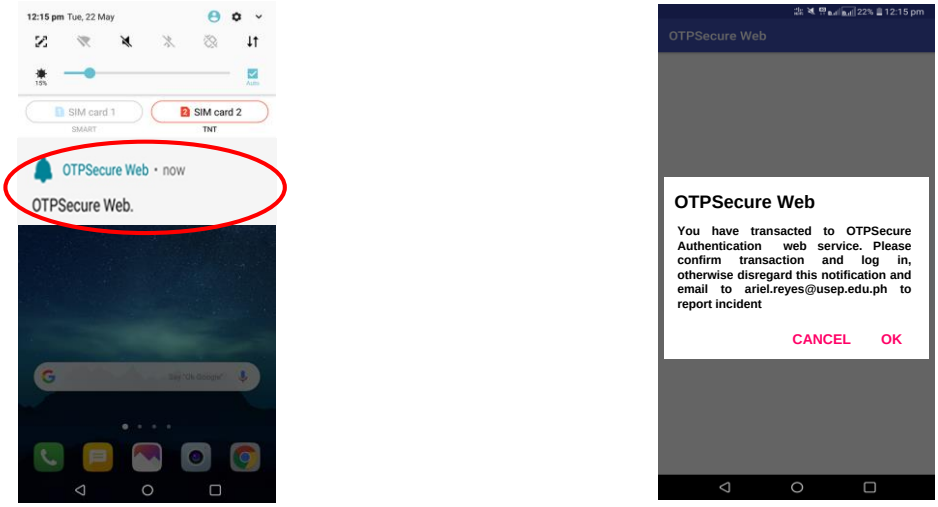
Table 1 Brute-force Cracking Estimated Time and Dictionary Attack Check Comparison

	Cracking Time Estimate (years)						Dictionary attack status
	Standard Desktop PC	Fast Desktop PC	GPU	Fast GPU	Parallel GPUs	Medium size botnet	
Proposed Architecture generated OTP (Blowfish-128 encrypted OTP)	About 244 decillion years	About 61 decillion years	About 24 decillion years	About 12 decillion years	About 1 decillion year	About 244 octillion years	Safe!
Plain Text OTP	0	0	0	0	0	0	Unsafe!

As shown in Table 1, unlike the plaintext OTP where brute-force and dictionary attacks were not necessary, the generated OTP of the proposed architecture required much greater time to determine its equivalent verification code. It can, therefore, be considered resilient against brute-force attack and is safe against a dictionary attack. The results of Crypto Bench and Crack Station also revealed that the generated OTP was not recognized to be any of the popular hash types supported by both tools.

5.2. EUA simulation result

EUA, in this study, was tested and evaluated under the following conditions. It should be able to capture SMS message coming from specific mobile number, can notify the user of the said SMS message, process the incoming message by performing XOR operation between the received message against the User ID, and send SMS message to WBA's mobile number. It was developed using Android Studio and was tested with the aid of another mobile phone, responsible for sending encrypted OTP and receiving new OTP from the end user. In testing EUA, users were asked to log in with WBA to acquire OTP on user's registered mobile number via SMS. Evaluation of the outlined conditions was observed after the user's login with WBA. Results revealed that WBA was successful in the determination of the authenticity of the user according to the user's registered mobile phone number, user ID, and the verification code/OTP.



(a) Notifications (b) Confirmation

Fig. 5 EUA Interface

The EUA component played a vital role in the process of securing the OTP/verification code in this architecture. It was responsible for notifying users of incoming SMS messages received from WBA. Whenever the user received an SMS message from WBA, a notification appeared on the screen informing the user of the transaction with the WBA (Fig. 5(a)). Detailed instructions along with a warning message were displayed after tapping the notification that allows user's confirmation as shown in Fig. 5(b).

Confirmation of the transaction was accomplished by pressing the OK button (Fig. 5(b)) that resulted in the creation of the new OTP. New OTP was produced through an XOR operation between the encrypted OTP and the user ID and was sent back to WBA via SMS as a reply, thus, performing end-to-end OTP. The new OTP was also subjected to the same test as the generated OTP to determine new OTP's security strength assuming that it was illegitimately acquired by adversaries during transmission from EUA to WBA. Results revealed the same findings referring to estimated cracking time and dictionary attack as shown in Table 1. It had also shown no match as compared to any of the popular hash types supported by Crypto Bench and Crack Station. These results guaranteed tighter security despite the worst scenario were adversaries acquire illegitimate access on the new OTP.

6. Contributions

Several works were introduced to secure OTP on OTP-assisted transactions as discussed in Section 3. Shown in Table 2 is the summarized assessment of these works and that of the proposed architecture whether or not they are susceptible to identified threats cited in the literature and other related weaknesses.

As presented in Table 2, the enhancements introduced in this work addressed the vulnerabilities with OTP-enable transactions. The proposed architecture get rid of VCFA and SMiShing through OTP protection. OTP was protected by not

making it available to users and through OTP encryption using Blowfish-128 algorithm. This approach made forwarding of a verification code to attackers hopeless and access to information nearly impossible even during the worst scenario where the verification code/OTP falls to the illegitimate user. The brute-force estimated cracking time showed that even OTP is acquired illegitimately either during transmission or after receipt of OTP, greater time is required to extract the verification code making it brute-force resilient. Eavesdropping accomplished through Key Logging, Screen Capturing, Shoulder Surfing, and related attacks were also eliminated by not engaging to manual entry of verification code through onscreen of physical keyboards, instead, the user application does the processing by merely asking user's confirmation in real-time. Another security issue known as server spoofing was further addressed through mutual authentication using end-to-end OTP for transaction confirmation between the application server and the user application and with the aid of real-time verification and authentication using users' registered mobile number, user ID, and the OTP. These developments guaranteed stronger security even on existing untrusted communication channel. Thus, making relevant information such as verification code indecipherable at lower implementation cost while promoting a more secure OTP for multifactor out-of-band authentication against social engineering practices enabled attacks and its related vulnerabilities.

Table 2 Summary of Threats Susceptibility Assessment on Various Works

Related Works	Attacks and Vulnerabilities						Other Requirement
	SMiShing	VCFA	Eavesdropping	Brute-force		Server Spoofing	
				In Transit	Receiver End		
[15]	YES	YES	YES	NO	YES/Not Necessary	NO	NONE
[6]	YES	YES	YES	NO	YES/Not Necessary	NO	NONE
[16]	NO	NO	NO	NO	NO	YES	Secure Channel
Proposed Architecture	NO	NO	NO	NO	NO	NO	NONE

7. Conclusions and Future Works

In this study, a solution was introduced to provide tighter security against SMiShing, Eavesdropping, and other related vulnerabilities accomplished through keylogging, screens capturing, shoulder surfing, and other social engineering practices for SMS-based OTP multi-factor authentication. Simulation results revealed that the proposed solution was free from the said vulnerabilities at minimal processing time required. It also revealed a higher level of security through end-to-end OTP implementation, thus, promoting a safer virtual world and making it more suitable for applications where security and privacy, as well as processing time, is highly essential such as that for SMS-based OTP multi-factor authentication systems. To further determine its performance and applicability, it is therefore recommended to first implement and test the proposed architecture on real-world online applications with not so sensitive tasks before wide-scale implementation. It is also recommended to use widely accepted method for generating OTP and key for additional security and to expand its capability to cater other mobile phone OS such as IoS and Windows to make it available to every user. Finally, services of bulk SMS provider should also be considered to ensure seamless delivery of encrypted OTP via SMS.

Conflicts of Interest

The authors declare no conflict of interest.

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.
[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. Sediyono, 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/