

Security approach for instant messaging applications: viber as a case study

Mohammed Falih Kadhim¹, Adel Al-Janabi², Ahmed Hazim Alhilali¹, Nabeel Salih Ali¹

¹Information Technology Research and Development Centre, University of Kufa, Najaf, Iraq

²University of Kufa, Najaf, Iraq

Article Info

Article history:

Received Oct 12, 2021

Revised Mar 6, 2022

Accepted Mar 15, 2022

Keywords:

Data security

Instant messaging

Privacy

Security

User privacy

Viber

Web applications

ABSTRACT

A variety of internet-based applications are widely used in our animation activities because they provide free and useful services. These applications, such as instant messaging, can be run via the web, mobile, or computer-based devices. Therefore, the security and privacy of user data over these apps have been concerned in recent years because of sensitive and confidential information considerations. Consequently, many instant messaging applications, like Viber, have various security and privacy issues that need to be understood and resolved. Viber users reached 800 million, and they increased dramatically due to the efficient services that this app provides. Hence, a loophole in an application's design may allow illegal access to the app and gain confidential and sensitive data. In this article, we proposed a security approach for Viber to safeguard user confidential data and sensitive information. The proposed approach involves two theoretical solutions: Short message service (SMS) authentication code and the physical hardware number to prevent illegal access to user data. Several scenarios are adopted to assess the proposed approach and achieve security and privacy for the user information.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adel Al-Janabi

University of Kufa

Iraq

Email: adelh.aljanabi@uokufa.edu.iq

1. INTRODUCTION

Currently, the use of smartphones has increased dramatically, and instant messaging (IM) apps have become a necessity for users. Many companies offer free instant messengers with outstanding features such as texting, phone calls, videos, and file sharing. Therefore, the security and privacy of data collected by these applications have recently become a concern due to sensitive and confidential information considerations.

In the digital era, different internet-enabled applications that offered free and efficient services have been used widely by people [1]. The most popular apps are IM applications, which offer access to online services and can be run via the web, mobile, and computer-based devices [2], [3]. Also, these apps allow us to exchange information in real-time via text messaging, voice messaging, and file sharing [4]. Sutikno *et al.* [5], instant message users worldwide reached 3.8 billion at the end of 2020. However, like other conventional technologies, instant messaging services have also been used to commit fraud, spread malware, hack users' personal information, and doing acts that violate the law [6]. Zhang *et al.* [7] mentioned that ordinary people use instant messaging applications in their daily communication [8].

On the other hand, terrorists have employed instant messaging for machinating terroristic attacks since the information encryption function has applied in Instant Message, which prevents them from being watched. Besides, children who have less knowledge of using IM may publish personal information that

could harm them or their families [9]. Besides, the poor design, configuration faults, or weakness in the written code for these applications, make them frequently vulnerable to attacks and theft user sensitive and confidential information [10]. Thus, the security and privacy of user data over these apps have been concerned in recent years because of sensitive and confidential information considerations. Hence, there are various instant messaging applications, like the Viber app, which suffers from multifarious security and privacy problems chat applications, with over 800 million registered users on its platform. After Edward Snowden revealed surveillance systems' existence, the majority of users have concerns about unreliable communication. However, many people still liked insecure instant messages applications because there is no instant messenger that could satisfy all the users' preferences.

Different studies presented many indicators that related to the consumers' concerns of using their data such as data collection users' awareness, misuse of data, internet user experience, and consumers' level of learning [11]. Schrder *et al.* [12], many companies collect, sell, and/or exchange the users' data with other companies or individuals for commercial or educational purposes. Also, Seghiri and Belguidoum [13] and Kadhim and Gaata [14] shows that several companies work on the internet to collect personal data and use it to make a profit. A study by Unger [15] discuss that based on the evaluation security process of nine IM applications that have done, the results confirm that most of these applications have major security flaws, which make them prone to various kinds of attacks [16], [17]. Moreover, an article has done by two researchers revealed that IM server owners could access the personal data of their customers when they want [18]. Also, an article by Ögüt *et al.* [19], presents hackers can retrieve user data that includes sent and received messages, photos, and other files from the mobile phone if they have physical access and proper software [20]. Many published papers noted that most of the social media applications, including IM, violate user privacy and unsafe to a different type of vulnerabilities. The authors listed the weaknesses, which include passwords revealing and store private information on the application server [21], [22]. However, the majority of the articles and researches that studied the security of IM applications have only evaluated their safety according to experiment and lab setups [23]. They neither describe the chat application structure and do not propose any solution and design to secure those applications [24], [25].

The proposed method can be described in the following section starting with analyzing and discussing the vulnerability and framework on how to fix it. Upon successful installation and activation of Viber on a Windows-based PC, user data containing encrypted credentials are generated inside the roaming folder that can be accessed via user's application data. This data allows the user to open Viber without having to re-enter credential every single time. However, this had also led to a significant security flaw that enables access to any Viber account if the victim's computer is not adequately protected.

The folder that Viber creates, which stores the account data is named ViberPC. When the created folder is copied to another computer which also has Viber installed, the victim's account will immediately open once the Viber app is run. Exposing contacts and messages without any authentication process unlike other instant messaging apps like WhatsApp, which requires QR code to be scanned by the phone during the first-time run and when data files are copied to another PC. Figure 1 presents a typical scenario demonstrating the vulnerability in the Viber instant message application, and Figure 2 shows a flowchart which showing the steps to activate the vulnerability.



Figure 1. Typical scenario demonstrating the vulnerability

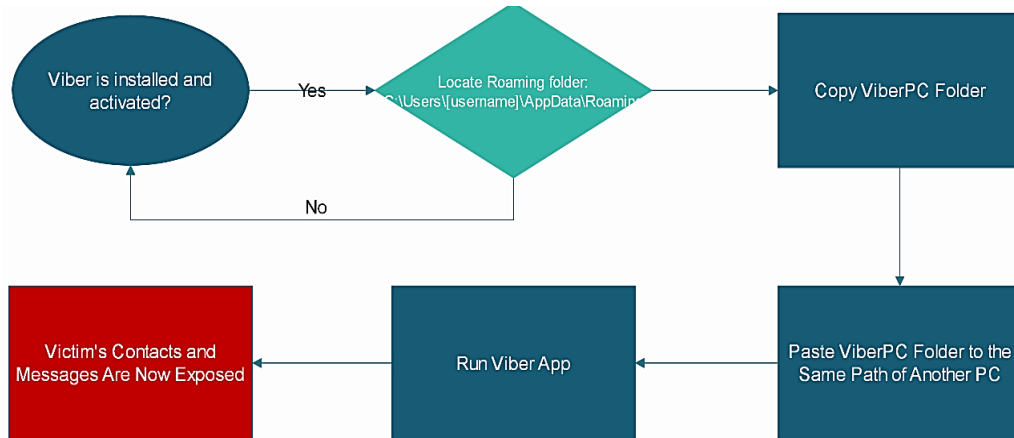


Figure 2. Flowchart showing the steps to activate the vulnerability

2. PROPOSING APPROACH

Two theoretical methods are proposed in this paper that should fix the application vulnerability. Admittedly, due to the nature of the following solution, it has not been tested as it requires direct modifications to the software which can only be done by the developing company. This can also be seen as a limitation of this study.

2.1. Authentication message method

In this method, triggers an authentication request in the form of a message every time the application starts. When the user launches the Viber App on PC, a message is sent to the Viber App on the user's mobile phone containing an activation code. The user has to enter the code to launch the Application and see contacts and messages. The app will stay active until it closes or the PC restarts. Figure 3 discuss the authentication message fixing algorithm.

```

Algorithm Authentication Message or QR
Run Viber app
Authentication =send a message to application Viber in mobile or QR
If Authentication then
    Lunch Viber App on pc
Else
    Access denied
End if
End Algorithm
  
```

Figure 3. Authentication message fix

2.2. Storage media serial number

This method relays on the storage media hardware such as the internal hard disk drive (HDD). The HDD and most storage media have a built-in serial number assigned from the industry during the manufacturing process. No identical serial numbers among these hardware units exist even the same company and model made it.

The authentication stage in the proposed method is triggered every time the application launches. First, it checks if this is the first time the application starts. If the answer is yes, the installation process usually commences, and it is finalized with registering the serial number of the HDD or whatever the user uses storage hardware. In the other hand, if the application has already been launched before then, it compares the serial number that was registered during the installation process with the current serial number of the HDD. If both values are identical, the application usually starts. Otherwise, an error message appears on the screen that requires to re-install the application by the user. Figure 4 presents the algorithm to storage media serial number fixing to prevent illegal access to the user account by the crafter.

```

Algorithm Storage Media Serial Number
Run Viber app
If First time run then
  Complete installation typically and register storage serial number hard disk
  Lunch Viber App on pc
Else
  If Check (number serial hard disk) then
    Lunch Viber App on pc
  Else
    Access denied
  End if
End if
End Algorithm

```

Figure 4. Storage media serial number fix

3. RESULTS DISCUSSION AND ANALYSIS

Two scenarios have been designed to evaluate the proposed security methods. The first one (vulnerability case) represents the current status of the Viber application; when the ViberPC folder copied to another computer, which has Viber installed, the victim's account will immediately open once Viber app is running. As a result, the victim's account will be monitored, and all the sent and received messages, photos, and data will appear in the other pc Figure 5.

The second scenario describes the protected status when the two proposed protection methods are applied. In the first method, the victim will be notified with SMS that has an activation code to ensure unauthorized people have no permission to launch the Viber application account. The other approach will check the stored HDD serial number, which registered on the Viber servers at the installation process before if both numbers matched Viber regularly launched; otherwise, access will be rejected Figure 6.

Two theoretical solutions proposed in this paper that require authentication to be made every time the application start. The first method involves SMS to be sent containing authentication code to the phone number that previously used to register the account. When the code is entered, Viber will start usually. Despite the high level of security involved in this approach, admittedly, it can be less practical as the authentication process is required every time the application is launched, which can also be cumbersome.

The other, more practical, method utilize hardware real number, which is unique and given by the manufacturer to every storage hardware. The storage media serial number cannot be masked or altered as it is burned within the hardware circuitry. Furthermore, this approach can be more practical as the authentication is done automatically within the software side without requiring human interaction. Once the authentication process is complete, Viber will be launched, and user data will be loaded. One major challenge in this paper is the lack of practical approval of the proposed solutions. Due to the closed source nature of the application, it is impossible to modify the source code of Viber to implement and examine the solutions illustrated in this research.

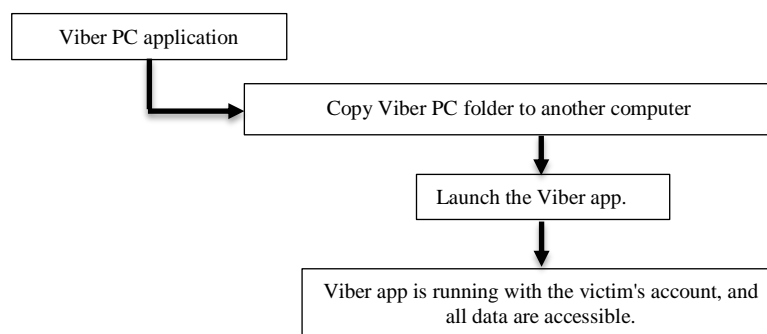


Figure 5. Not protected scenario

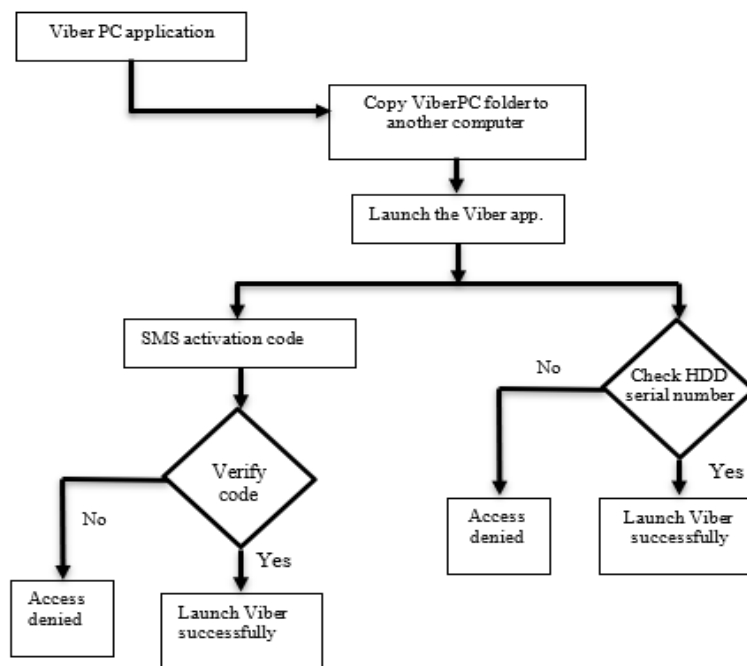


Figure 6. Protecting approach

4. CONCLUSION

The rapid increase in popularity of the instant messaging application, Viber, in recent years, has led to security challenges that need to be addressed to protect the privacy of millions who use this application. This paper focuses on a significant vulnerability that hackers can take advantage of to gain access to all personal data of the victim quickly. Upon critical analysis, the data folder that Viber creates after successful installation ones copied to another PC, the victim's personal data will be exposed and can be viewed by the hacker. This is due to the lack of proper authentication when the application starts. This paper proposes two theoretical solutions that require authentication to be made every time the application starts. In the first method, the user will get an SMS message containing an authentication code to the phone number previously used to register the account. While in the second method, the authentication is done automatically within the software side without requiring human interaction by utilizing the hardware's actual number. In conclusion, protecting user's privacy and security should always be given high priority in any software, especially those that personal store data, pictures, or videos. As long as the user data is stored locally, unprotected and unencrypted on the computer, gaining access to these data might will not be difficult even for an intermediate hacker. It is vital to prevent access to personal data employing authentication processes to confirm the identity of the user before making the data accessible.




REFERENCES

- [1] A. Al Farawn, H. D. Rjeib, N. S. Ali, and B. Al-Sadawi, "Secured e-payment system based on automated authentication data and iterated salted hash algorithm," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, pp. 538–544, Feb. 2020, doi: 10.12928/TELKOMNIKA.V18I1.15623.
- [2] N. S. Ali, "A four-phase methodology for protecting web applications using an effective real-time technique," *International Journal of Internet Technology and Secured Transactions*, vol. 6, no. 4, p. 303, 2016, doi: 10.1504/ijitst.2016.10003854.
- [3] P. Ahluwalia, U. Varshney, K. S. Koong, and J. Wei, "Ubiquitous, mobile, pervasive and wireless information systems: Current research and future directions," *International Journal of Mobile Communications*, vol. 12, no. 2, pp. 103–141, 2014, doi: 10.1504/IJMC.2014.059738.
- [4] M. H. Alattar, A. Al Farawn, and N. S. Ali, "Anti-continuous collisions user-based unpredictable iterative password salted hash encryption," *International Journal of Internet Technology and Secured Transactions*, vol. 8, no. 4, pp. 619–634, 2018, doi: 10.1504/IJITST.2018.095944.
- [5] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. Much Ibnu Subroto, "WhatsApp, Viber and Telegram which is best for instant messaging?," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 3, p. 909, Jun. 2016, doi: 10.11591/ijece.v6i3.pp909-914.
- [6] T. Y. Yang, A. Dehghantaha, K. K. R. Choo, and Z. Muda, "Windows instant messaging app forensics: Facebook and Skype as case studies," *PLoS ONE*, vol. 11, no. 3, p. e0150300, Mar. 2016, doi: 10.1371/journal.pone.0150300.
- [7] L. Zhang, Q. Ji, and F. Yu, "The security analysis of popular instant messaging applications," in *2017 International Conference on Computer Systems, Electronics and Control, ICCSEC 2017*, Dec. 2018, pp. 1324–1328, doi: 10.1109/ICCSEC.2017.8446863.




- [8] A. S. Bin Shibghatullah, H. K. Fatlawi, S. Kadhim, M. Falih, N. S. Ali, and A. H. Alhilali, "A comparative analysis and performance evaluation of web application protection techniques against injection attacks," *International Journal of Mobile Communications*, vol. 18, no. 1, p. 1, 2020, doi: 10.1504/ijmc.2020.10019530.
- [9] P. Dashtinejad, "Security system for mobile messaging applications," *diva portal*, 2015, [Online]. Available: <http://www.diva-portal.org/smash/get/diva2:813095/fulltext01.pdf>.
- [10] A. S. Tsioulos and G. M. Giaglis, "Mobile websites: Usability evaluation and design," *International Journal of Mobile Communications*, vol. 12, no. 1, pp. 29–55, 2014, doi: 10.1504/IJMC.2014.059241.
- [11] I. Paspatis, A. T. A. Tsohou, and S. K. S. Kokolakis, "Mobile application privacy risks: Viber users' de-anonymization using public data," in *Mediterranean Conference on Information Systems (MCIS)*, 2017.
- [12] S. Schrder, M. Huber, D. Wind, and C. Rottermann, "When SIGNAL hits the Fan: On the Usability and security of state-of-the-art secure mobile messaging," in *Proceedings 1st European Workshop on Usable Security*, 2017, doi: 10.14722/eurosec.2016.23012.
- [13] H. Seghiri and R. Belguidoum, "Development of a secure messaging app for android mobile," Dissertation, Dept. Computer Science, Mohamed Boudiaf University, 2021.
- [14] R. W. Kadhim and M. T. Gaata, "A hybrid of CNN and LSTM methods for securing web application against cross-site scripting attack," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, pp. 1022–1029, Feb. 2020, doi: 10.11591/ijeecs.v21.i2.pp1022-1029.
- [15] N. Unger, "End-to-end encrypted group messaging with insider security," *European Workshop on Usable Security*. IEEE, 2021.
- [16] P. K. Aggarwal, P. S. Grover, and L. Ahuja, "Security aspect in instant mobile messaging applications," in *IEEE International Conference on 2018 Recent Advances on Engineering, Technology and Computational Sciences, RAETCS 2018*, Feb. 2018, pp. 1–5, doi: 10.1109/RAETCS.2018.8443844.
- [17] N. A. Rahman, F. I. M. R. Syamil, and S. B. b. Rodzman, "Development of mobile application for Malay translated hadith search engine," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 2, pp. 932–938, Nov. 2020, doi: 10.11591/ijeecs.v20.i2.pp932-938.
- [18] O. S. Adebayo, J. S. Anyam, S. Ganiyu, and S. A. Salawu, "Analysis and classification of some selected media apps vulnerability," in *Communications in Computer and Information Science*, vol. 1350, 2021, pp. 457–469.
- [19] N. D. Ögüt, Ç. Ögüt, and P. Eşme, "The role of online consultation requests to personal social media accounts and instant messaging services of dermatologists in occupational burnout: An emerging problem," *Journal of Cosmetic Dermatology*, 2021, doi: 10.1111/jocd.14417.
- [20] P. M. M. Govind, "The effect of technology-based instant messaging applications on employee engagement," Master Thesis, University of Pretoria, 2021.
- [21] E. B. Sorensen, "Using static analysis to detect vulnerabilities in OpenID connect clients," Master Tesis, NTNU, 2020.
- [22] A. Al-Janabi, E. A. Al-Zubaidi, and R. H. A. Al-Sagheer, "Encapsulation of semantic description with syntactic components for the Arabic language," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 961–967, May 2020, doi: 10.11591/ijeecs.v22.i2.pp961-967.
- [23] I. Vaccari, S. Narteni, M. Mongelli, M. Aiello, and E. Cambiaso, "Perpetrate cyber-attacks using IoT devices as attack vector: The ESP8266 use case," *CEUR Workshop Proceedings*, vol. 2940, pp. 35–46, 2021.
- [24] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, "A frictionless and secure user authentication in web-based premium applications," *IEEE Access*, vol. 9, pp. 129240–129255, 2021, doi: 10.1109/ACCESS.2021.3110310.
- [25] J. Huang, J. Zhang, J. Liu, C. Li, and R. Dai, "UFuzzer: Lightweight detection of PHP-based unrestricted file upload vulnerabilities via static-fuzzing co-analysis," in *ACM International Conference Proceeding Series*, Oct. 2021, pp. 78–90, doi: 10.1145/3471621.3471859.

BIOGRAPHIES OF AUTHORS






Mohammed Falih Kadhim    is the directing manager of Software department at ITRDC, University of Kufa. He and his team are responsible for developing and administrating all websites in the University and its' faculties. Earned his bachelor degree in Computer Technique Engineering from the Islamic College University in 2010. Later, he earned his Master degree in Information Technology from the University of Technology, Sydney, Australia in 2015. His research interests are mostly Network and web related such as Front-end Web Development, WSN, Learning Management Systems, Peer-learning using Social Media Platforms. He can be contacted at email: mohammed.kadhim@uokufa.edu.iq.






Adel Al-Janabi    Received the BSc. in computer science from University of Babylon, Iraq and the MSc in Computer Science from Southern Russian state polytechnical university (NPI) of M. I. Platov, Russia. His research interests include the applications of Artificial Intelligence, Image processing, Security and Natural Language Processing. He can be contacted at email: adelh.aljanabi@uokufa.edu.iq.



Ahmed Hazim Alhilali    Received the BSc. Degree in computer science from Imam Ja'afar Al-Sadiq University in Computer Science in 2009 and the Master degree in Information Technology from the University of Technology Sydney, Sydney, Australia, in 2016. He can be contacted at email: ahmed.alhilali@uokufa.edu.iq.



Nabeel Salih Ali    Received his the BSc. in Computer Science from the University of Technology, Baghdad, Iraq, in September 2003, and the MSc. in Computer Science (Internetworking Technology) from the University Technical Malaysia Melaka (UTeM), Malaysia, in July 2015. He works as a deputy for director of ITRDC centre for scientific affairs and manager of the scientific research division at ITRDC centre and Lecturer in Faculty of Engineering, Faculty of Education, and Faculty of Education for girls at the University of Kufa. His research works in Computer Networks and Security. Besides, Healthcare Monitoring Systems, the Internet of Things (IoT), Machine Learning (ML), and Brain-Computer Interface (BCI). He can be contacted at email: Nabeel@uokufa.edu.iq.