OPEN ACCESS

Research Paper

WhatsApp Web QR code: Auto-change Frequency Analysis

[1] Department of Electronics and Telecommunication, Gangadhar Meher University, Odisha, India

* lbkb.edu@gmail.com

Lalatendu Bidyadhara Kumar Barik[1*], Nikita Barik[1]

ABSTRACT

Purpose: The purpose of the study is to investigate the behavioral aspects of WhatsApp Web QR code and its impact on privacy of users. **Background:** WhatsApp is the fastest growing private online chat network for encrypted messaging. The role of QR code encryption in WhatsApp Web interface provide users with the ability to secure communication. It remains uncertain if the same trends occur in the encryption protocol. To strengthen user's security and privacy, the cryptographic algorithm has been modified to protect from the attackers. **Methodology:** The research was performed over a span of four months (July-October 2020) on experimental basis in India. All the observations and measurements were carried out using Mozilla Firefox web browser and the open source screen recording tool i.e. CamStudio. QR code decoding was performed in the ZXing decoder environment. **Findings:** This research examined the auto-change scale factor of the QR code in WhatsApp Web (A browser-based application of WhatsApp). The findings revealed that the QR code auto-change factor is 20 seconds while the QR code reload factor is 120 seconds. Evaluations showed that six consecutive QR code variations take place over each QR code reload period. Upon decoding the QR code of each set of QR code reload period, we observed that the parsed result of all QR codes were different. Each set of QR code reload period has six unique QR codes; even that doesn't match the QR codes of the subsequent sets. Randomly changing QR codes are due to cryptographic algorithm that provides users for secure authentication and end-to-end-encryption.

Keywords:
QR Code, WhatsApp Web, Scale of Auto-change, Scale of Reload

1. INTRODUCTION

Security is the most vital factor in the cyber world. Day-by-day with expanded connectivity via internet technologies, the user needs more privacy throughout the wall. To accomplish these needs, users are more focused on using convenient, stable and secure messaging applications. WhatsApp, a mobile-based application, is consistently increasing in popularity among users across the globe due to its security and privacy features. Nowadays, over 2 billion monthly active users (MAUs) are using the popular WhatsApp messaging app (Clement, 2020). The increasing popularity of WhatsApp messenger among users is due to its end-to-end encryption (E2EE) protocol (WhatsApp, 2016). All the communication including chats (personal or group chats) and files (images, documents, videos, voice messages) are protected with end-to-end encryption protocol. Due to this end-to-end encryption, no third parties even WhatsApp can't read the messages of users; however the messages can only decrypted by the recipient user.

مجلة دراسات المعلومات والتكنولوجيا
جمعية المكتبات المتخصصة
فرع الخليج العربي
JIST-SLA-AGC

https://doi.org/10.5339/jist.2021.10

Submitted: 25 October 2020
Accepted: 16 December 2020
Published: 30 September 2021

كيوساينس
QSCIENCE
دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

Cite this article as: Barik LBK, Barik N. WhatsApp Web QR code: Auto-change Frequency Analysis. Journal of Information Studies & Technology 2021:2.10. https://doi.org/10.5339/jist.2021.10

WhatsApp provides two flavors to users i.e. WhatsApp Web and WhatsApp Desktop to use on the computer. WhatsApp Web is a browser-based application of WhatsApp. It is the computer-based extensions of WhatsApp account on the user's phone. Moreover, WhatsApp Web provides a platform to the WhatsApp users to use the app through browsers. To avail this browser-based feature, the user must connect to WhatsApp Web through WhatsApp application by scanning the Quick Response (QR) code. The messages that user send or receive are synced between the user's phone and the computer. The user can see the sent or received messages on both devices – user's phone as well as on computer.

Increased popularity of over-the-top (OTT) messaging over the past decade, WhatsApp is one of the effective cross-platform mobile instant messaging (MIM) application on the market (Tawiah et al., 2014). WhatsApp is the most popular messaging application (Sutikno et al., 2016) that Facebook acquired in 2014. For messaging, WhatsApp requires internet connectivity on both parties (sender and receiver) devices and the software must be installed on their mobiles. The social media platform especially WhatsApp messenger has become a dominant influence in today's digital era (Tawiah et al., 2014). WhatsApp may contribute to significant changes in the lives of users, but may at the same time trigger severe social and personal issues, including the addiction towards the app (Chahal et al., 2015). Tough messaging apps have been around for a number of years, the evolution of secure messaging apps has been increasing; emphasizing on protecting the privacy of users and meeting their needs (Corpuz, 2020; Das, 2020). Recent studies have shown that users are becoming more concerned about protecting privacy on their smartphones and opposed applications (Apps) that collected their contacts (Balebako et al., 2013).

Some authorities and governments are hacking mobile devices to gain unauthorized access for surveillance purposes and for other unknown reasons (Curran, 2018). As reported in India Today (Ganjoo, 2019), "Indian government has asked WhatsApp to digitally fingerprint all its messages. Digitally fingerprinting messages would enable traceability of messages on WhatsApp. India government wants WhatsApp to trace origin of message without seeing its contents." India's plan to mandate the monitoring, interception and tracing of messages on WhatsApp breaches the privacy of users. Fortunately, WhatsApp refused government of India's demand to trace the origin of message. The signal protocol developed by Open Whisper System provides end-to-end encryption for instant messaging (Marlinspike, 2014). In 2016, WhatsApp utilized signal protocol to strengthen the security and privacy of users.

As per version 1.0 Secure Messaging Scorecard released by the Electronic Frontier Foundation (EFF), WhatsApp got 6 point out of 7 (EFF, 2014). The seven criteria from which EFF released the score card are as follows:

- Criteria – 1: Encrypted in transit?
- Criteria – 2: Encrypted so the provider cannot read it?
- Criteria – 3: Can you verify contact's identities?
- Criteria – 4: Are past communications secure if your keys are stolen?
- Criteria – 5: Is the code open to independent review?
- Criteria – 6: Is security design properly documented?
- Criteria – 7: Has there been any recent code audit?

Based on these seven aspects WhatsApp fails the criteria of open independent review of source codes. Until now WhatsApp does not release all the source codes but some of them are openly available in GitHub page of WhatsApp.

Table 1. EFF's Version 1.0, secure messaging scorecard illustrations of WhatsApp (Source: EFF, 2014)

Secure Messaging Scorecard of WhatsApp						
Criteria – 1	Criteria – 2	Criteria – 3	Criteria – 4	Criteria – 5	Criteria – 6	Criteria – 7
☑	☑	☑	☑	☒	☑	☑

Billions of people downloaded WhatsApp from Google Play Store on Android devices. The current download statistics (dated 18 October, 2020) showed that this App has been downloaded 5,000,000,000+ times. Apart from this, WhatsApp needs certain permissions from users to operate like contacts, camera, location, call logs, phone, SMS, storage etc. These permissions can be abused, it is questionable! Apart from personal instant messaging, WhatsApp lunched WhatsApp Business

API for solutions of small, medium and large-scale businesses to provide communication with customers globally. This research examined the security scheme, cryptographic architectural aspects of WhatsApp Web.

2. MATERIALS & METHODS

After a preliminary study was conducted to ensure that all the requisite hardware and software components installed were operating efficiently; the experiment was conducted over a span of four months (July – October 2020). The research focused on auto-changing frequency measurement of the WhatsApp Web QR code. The experimental ecosystem is an HP 241 G1 Notebook that operates a 64-bit Windows 10 operating system with Mozilla Firefox browser v78.0.1 (64-bit) installed. CamStudio software v2.7 is used for precise measurement of time elapsed. The ZXing open source decoder is used to decode the QR code. The Android smartphone ASUS Zenfone Max M1 (ASUS_X00PD) that is installed with Android operating system v8.0 and an active WhatsApp account (running WhatsApp messenger v2.20.193.9) is used for checking login session. The WhatsApp Web is accessed through the Firefox browser with active internet connectivity.

The WhatsApp Web interface has QR code with encoded information that helps users to enter the web-based features by scanning the code via WhatsApp on their phones. The messages that users send are end-to-end encryption with combination of asymmetric RSA and symmetric AES algorithm. Due to this cryptographic algorithm, the privacy of users are maintained throughout the WhatsApp medium.

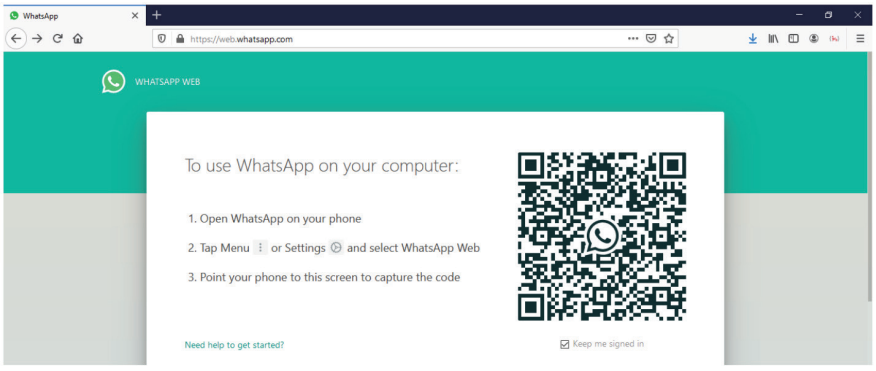

Figure 1. WhatsApp Web Interface (Source: https://web.whatsapp.com)

It was observed that the QR code in WhatsApp Web automatically changed to a new QR code after a certain interval of time. This is because of the cryptographic encryption algorithm and to prevent the hackers and attackers to access the user's behavior. The reloading time of the next set of QR codes depends on the authentication time of the user. If the user scans the WhatsApp Web QR code during the QR code reload period, the user gets authentication and enters the WhatsApp Web login session.

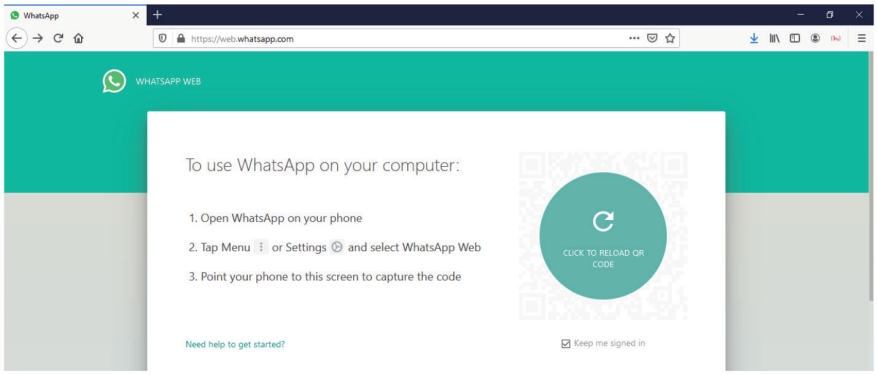

Figure 2. WhatsApp Web Interface showing 'CLICK TO RELOAD QR CODE' (Source: https://web.whatsapp.com)

The time period between first appearance of QR code and 'CLICK TO RELOAD QR CODE' message in WhatsApp Web interface is called the QR Code Reload Period (QR-CRP). The scale of time describing QR-CRP is known as QR Code Reload Factor (QR-CRF) and is denoted by τ_R. The time gap between auto-changing new QR codes within a single QR-CRP is called QR Code Auto-change Scale Period (QR-ASP). The scale of time describing QR-ASP is known as QR Code Auto-change Scale Factor (QR-ASF) and is denoted by τ_A. Fig. 3 shows the one single set of QR-CRP and its associated six QR-ASP.

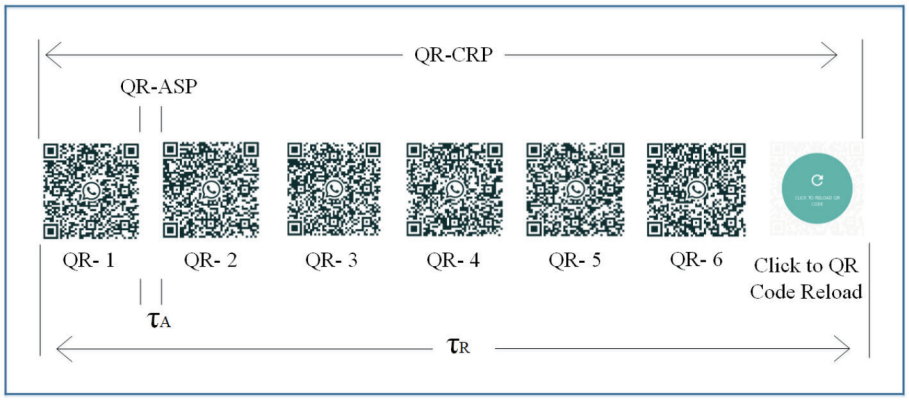

Figure 3. Representation of QR-CRP and QR-ASP cycle

Several observations have been taken to measure the time gap. During the first few trials we observed through naked eye. Due to observer view and parallax error the study encountered more errors during the first few attempts. Later on, we moved to open source screen recording tools (CamStudio) so that the measurement of the time gaps between each successive change of QR code could be done effectively and efficiently. By using software tools, the accurate measurement of the time gap in QR-CRP and QR-ASP was carried out.

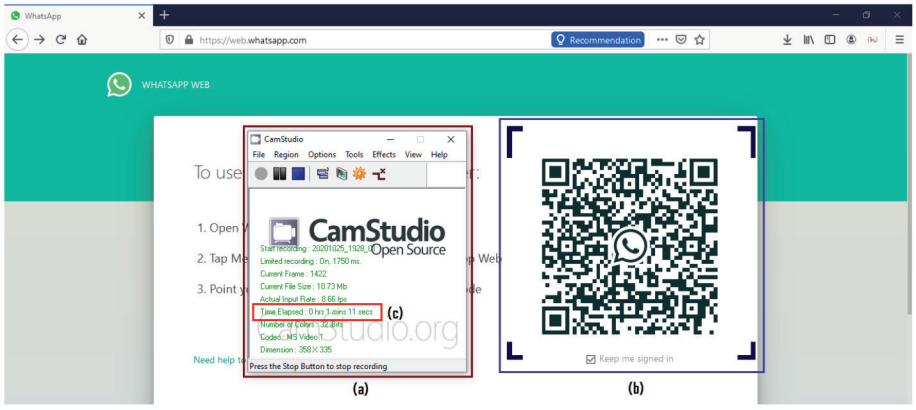

Figure 4. Measurement of QR-CRF and QR-ASF in WhatsApp Web interface [(a) Brown region represents the CamStudio recording environment, (b) Blue region represents the recorded area, (c) Red region represents the time period measurement].

3. RESULTS & DISCUSSION

This section presents the results of the testing processes as per the methods mentioned above. The results and discussion are based on the observations made in the experiment.

Thirty (30) samples of QR-CRP were evaluated and examined. It was observed that in a single QR-CRP there were six QR-ASP. This means, six new QR codes appears in WhatsApp Web interface automatically in a single QR-CRP. The auto-changing of QR code is due to preserving the secure protocol to provide authentic security to the users. The QR-ASF (τ_A) was found to be 20 seconds, whereas the QR-CRF (τ_R) was observed to be 120 seconds. Thus, we reached the conclusion that six QR-ASP constitutes a single QR-CRP in WhatsApp Web.

The decoding of QR codes was done through open source ZXing decoder, which showed that none of the QR codes have the same parsed result. The QR codes of each 30 samples set of QR-CRP had

different parsed result. None of the single QR code matched with each other. The WhatsApp Web QR codes were randomly generated by cryptographic algorithm to provide security to the users.

Table 2. Parsed results of QR codes of two sets of QR-CRP from WhatsApp Web using ZXing Decoder

QR-CRP – 1		
S.N.	**QR Code**	**Parsed Result**
QR-1		1@OkCy3mzWh5MPnFr9j30AbbicQ4EhBys8I8+kXjVPV2R/6JGI43Q2kDZXEkdXmVP60/wFkDt32+gprg==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-2		1@iRg+hqQamhpqNMXgX9uryJ3nlRjgzhGht/Wx9NS90ed37TBbecymaZLWU+fHBIf486FQk2TWAIKApw==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-3		1@x/B3sMVSvTjbpBKq4wfRqdoEyclAlLDJ7xIu/U+XdGJsGu2m63r74WnZwTmqFInHVvucLEBhsitfGw==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-4		1@f2CuIZ3qTB+DOwUwV548jxFh+vaiekMOlgB4HV3VnOJtdkHy1jo1EFVHtqk9hPXJo6sACHIyTcYhLQ==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-5		1@n14T3jWGjLogwb2Y95jaOjpyTf1gM/5tisvZe5n4iiDqGgp+XU3k5wU4LF19tpP7QztyCo1KS+G4Aw==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-6		1@mFTvAmPa6KyKH9QcUZS6D8usOhbos4P4NGYyRphRSuCdb/z5swRJEWyquzJhbRz1+Ece1KoVRakhOQ==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-CRP – 2		
S.N.	**QR Code**	**Parsed Result**
QR-1		1@6/VWNRUJMIhEwQDO6gj6x7KnC6W8TyNr/xRXzR9275tUqTvIgFxsBvsOILMhvV3SvuLw7hBJl3yeng==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-2		1@oY9BLW+XWM2oPs1hkxeBxFC80co8PYNIPiUCFsemwq/K/yjWS2T5oH48fmhqb28GKys7DKssKHEK+Q==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-3		1@F4nRrnprN9Zi7VoSLuNQbFWdms+aBrA7rl2Pf1b4rmZRf3ez490unM46bkX8xhuKapkOxfzaVYeJmQ==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==

QR-4		1@6Fk5ZZYiE1QAR8YrotqqODLx8okf2Gpvid2rO5m8JTjyik3Jf1yQhRND9+n3c47bCQkjtPq+tUCZ5A==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-5		1@rpfsXau77rArk+Qjl2igqUhPdmqqekbLTrKVmu886VcslB5N+lDec7rt17yFH+G8arg6hEllYfPnEA==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==
QR-6		1@Ct1tst3ctuuU8lV4OAZXMXrnqguMeVOpMsGD5ja2QToTolo8S8+4f5ECOpBWwjC1csMdc/LD2Q2agw==,dd754FG2JOWiCnkHw76RQ+tJPST880x3aDRYjiKnrko=,2/hHkHOWoDyrtClVh7omkA==

4. CONCLUSION

WhatsApp uses end-to-end encryption protocol to strengthen the security among the users. In this paper, we studied the QR-CRP and QR-ASP for better understanding of auto-changing QR code feature of WhatsApp Web. The percentage of matching of QR codes in subsequent QR-CRP cycle is less than zero because it was observed in the study that in 30 samples none of them matched and were randomly changing due to cryptographic encoding algorithm. The auto-changing QR codes in WhatsApp Web prevents users from unauthorized access from attackers. Due to this, the WhatsApp Web provides a trustworthy interface to the WhatsApp users to access though computer and maintain the security.

REFERENCES

Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013). *"Little brothers watching you": Raising awareness of data leaks on smartphones*. Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS' 13), Association for Computing Machinery, New York, NY, USA, Article 12, pp. 1–11. https://doi.org/10.1145/2501604.2501616

Chahal, R., Kaur, J., & Singh, N. (2015). A study to analyze relationship between psychological behavioral factors on WhatsApp addiction among youth in Jalandhar District in Punjab. *The Journal of Social Sciences Research*, *1*(1), 1–5. https://ssrn.com/abstract=2810438

Clement, J. (2020). *Most popular global mobile messaging apps 2020, Statista (Online)*. Retrieved July 1, 2020, from https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Corpuz, J. (2020). *Best encrypted messaging apps*. Retrieved June 25, 2020, from https://www.tomsguide.com/reference/best-encrypted-messaging-apps

Curran, D. (2018). *Are your phone camera and microphone spying on you?* Retrieved June 25, 2020, from https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying

Das, A. (2020). *10 Best Secure and Encrypted Messaging Apps for Android & iOS*. Retrieved June 25, 2020, from https://fossbytes.com/best-secure-encrypted-messaging-apps/

Electronic Frontier Foundation. (2014). *Secure Messaging Scorecard, (Online)*. Retrieved July 1, 2020, from https://www.eff.org/pages/secure-messaging-scorecard

Ganjoo, S. (2019). *WhatsApp maintains its stand on govt's request for message traceability in India*. Retrieved June 25, 2020, from https://www.indiatoday.in/technology/news/story/whatsapp-maintains-its-stand-on-govt-s-request-for-message-traceability-in-india-1551098-2019-06-18.

Marlinspike, M. (2014). *Open Whisper Systems partners with WhatsApp to provide end-to-end encryption*. Retrieved June 25, 2020, from https://signal.org/blog/whatsapp/.

Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M. A., & Subroto, I. M. I. (2016). WhatsApp, Viber and Telegram which is best for instant messaging? *International Journal of Electrical and Computer Engineering (IJECE)*, *6*(3), 909–914. https://doi.org/10.11591/ijece.v6i3.10271

Tawiah, Y. S., Nondzor, H. E., & Alhaji, A. (2014). Usage of WhatsApp and Voice Calls (Phone Call): Preference of polytechnic students in Ghana. *Science Journal of Business and Management*, *2*(4), 103–108. https://doi.org/10.11648/j.sjbm.20140204.11

WhatsApp (2016). *WhatsApp encryption overview: Technical white paper*. WhatsApp Inc. Retrieved July 3, 2020, from www.whatsapp.com/security.