THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 2 Article 11

6-30-2017

Signatures of Viber Security Traffic

M.A.K. Sudozai
National University of Sciences and Technology, asad.khan@seecs.edu.pk

N. Habib
National University of Sciences and Technology, n386@gmail.com

S. Saleem
National University of Sciences and Technology, sajid.saleem@seecs.edu.pk

A.A. Khan
National University of Sciences and Technology, amir.ali@seecs.edu.pk

SIGNATURES OF VIBER SECURE TRAFFIC

M.A.K.Sudozai[1], N.Habib[2], S.Saleem[1], A.A.Khan[1]
National University of Sciences and Technology
Islamabad, 46000, Pakistan
{asad.khan, sajid.saleem, amir.ali}@seecs.edu.pk[1], {n386}@gmail.com[2]

ABSTRACT

Viber is one of the widely used mobile chat application which has over 606 million users on its platform. Since the recent release of Viber 6.0 in March/April 2016 and its further updates, Viber provides end-to-end encryption based on Open Whisper Signal security architecture. With proprietary communication protocol scattered on distributed cluster of servers in different countries and secure cryptographic primitives, Viber offers a difficult paradigm of traffic analysis. In this paper, we present a novel methodology of identification of Viber traffic over the network and established a model which can classify its services of audio and audio/video calls, message chats including text and voice chats, group messages and file/media sharing. Absolute detection of both parties of Viber voice and video calls is also demonstrated in our work. Our findings on Viber traffic signatures are applicable to most recent version of Viber 6.2.2 for android and iOS devices.

Keywords: Viber, Proprietary communication protocol, End-to-end encryption, Traffic analysis

1. INTRODUCTION

Viber is one of the popular mobile applications that allows its users to communicate securely through internet connectivity on 3/4 G or WiFi. It is a product of Rakuten Inc. (Rakuten, 1997 (accessed 9-November-2016)) and currently has more than 606 million users on its platform. Based on a complex structure of geographically distant servers, complete communication protocol of the Viber is not known. In current version of Viber, all of core features are secured with end to end encryption: voice and video calls, one-on-one messages, group messages and media sharing. No known attacks with promising success rate exist on used encryption algorithm, associated primitives used for authentication and key establishment protocols. Even the used keys for content encryption are generated in such a way that even Viber has no control over them and track to previously used keys or future keys doesn't exist in the design. In this scenario of strongly build security architecture, access to the contents of Viber during the transit over the network is not known to be possible.

Like any other chat or social media secure app, analysis of Viber has three dimensions; the strength analysis of security functions incorporated in the Viber, platform forensics hosting the app and black box traffic analysis between the client and their servers. First two dimensions are beyond the scope of this paper while third one is our focus here. The detailed analysis of the secure Viber traffic was conducted for different services offered by Viber and peculiar signatures of Viber traffic were identified even in a secure end-to-end encryption scenario.

The taxonomy of internet traffic can be combination of protocols, applications, websites, and services obscured in a defined byte patterns; data packets and associated layered headers. Even under the concealed arrangements of SSL driven HTTPS traffic, internet traffic follow certain pre-defined rules of data encapsulations related to different protocols/services and their headers.

In Viber communication protocol, pattern of secure connections to heterogeneous cluster of servers including Viber and Amazon cloud servers is very complex (Marik, Bezpalec, Kucerak, & Kencl, 2015). With such a scope where protocol details of communication between geographically distant located servers and their clients are not known, analysis of encrypted traffic becomes a real challenge. However, extensive study of network traffic, identification of protocols though enforced events, connectivity requests and their acknowledgments, activity related size of exchanged frames/ packets and fixed byte patterns were few of techniques used in combination to profile the encrypted traffic of Viber.

To reach from unknown to maximally possible known, a detailed analysis of Viber services was carried out in this paper. The communication between the Viber clients to their servers was studied through series of event driven scenarios and identification of Viber from the traffic flowing over a live network was made. The further classification of Viber traffic into text/chat messages, file sharing, voice and video sessions is successfully demonstrated in this paper.

The paper is organized as follows. Section 2 briefly covers the account of relevant work done so far on different dimensions of analysis of social media applications. Section 3 elaborates our main work in which mechanism of traffic interception, its filtering and identification of voice/video communication and chat conversation is given. The accurate detection flow and classification of each Viber service is summarized through a flow chart in this Section. Events of chat conversations studied in relation to payload sizes and results of their behaviour analysis is also described in this Section. The Paper is finally concluded in Section 4.

2. RELATED WORK

Traffic analysis of Internet has been a well studied area. The evolution of robust networks, new protocols and changing encapsulation techniques attracted the research community to carry out intensive studies for classification of network traffic (Chen, Jin, Cao, & Li, 2010), (F. Zhang, He, Liu, & Bridges, 2011), (J. Zhang, Chen, Xiang, Zhou, & Vasilakos, 2013) and (Callado et al., 2009). The detailed analysis of traffic classification, its historical context, breakthroughs achieved so far and technical reasons which are hindering the accuracy and effectiveness of classification techniques are summarized in (Dainotti, Pescape, & Claffy, 2012).

The actual problem of traffic analysis is converged to anonymity of networks (Gilad & Herzberg, 2012), encrypted contents (Coull & Dyer, 2014) and secure cloud based applications. Number of techniques of traffic analysis were introduced, like traffic flow records (Chakravarty, Barbera, Portokalidis, Polychronakis, & Keromytis, 2014), bandwidth estimations (Chakravarty, Stavrou, & Keromytis, 2010) and machine learning techniques (Nguyen & Armitage, 2008). A comprehensive survey of these classification techniques with a focus on encrypted traffic was conducted recently in (Velan, Čermák, Čeleda, & Drašar, 2015). In succession, several studies were carried out to profile the secure social media applications like Skype, Whatsapp, Viber, and Signal.

Being the pioneer in secure VoIP chat application, Skype received the focused attention of forensic community. Amongst the recent works, (Adami, Callegari, Giordano, Pagano, & Pepe, 2012) used both statistical test methods and signature based procedures to classify the signaling and data traffic including voice / video calls and file transfers. (Yuan, Du, Chen, Wang, & Xue, 2014) studied the UDP flows of Skype to correctly identify the Skype traffic over the network.

A recent promising work on analysis of 20 android apps covered three possible scenarios of data on device, data in transit over the network and data on server storage (Walnycky, Baggili, Marrington, Moore, & Breitinger, 2015). Evidentiary traces of passwords, screen shots, video, text messages audio, GPS location, profile pictures were found to be recoverable from

smartphone or exploitable by malicious actor over the network. Besides stored data forensics of apps, focus was on re-construction/ partial reconstruction of traffic through plain contents of these messaging applications.

WhatsApp, being the most popular choice in recent years, gained the maximum attention of forensic community. The most recent work was presented in (Karpisek, Baggili, & Breitinger, 2015) where authors analyzed network level traffic of WhatsApp and obtained its forensics artifacts. The start point of the analysis was from Whatpps API where authors were able to access mobile phone OS. Having access in a purely development environment, client-server communication was analyzed in detail. The sessions between the client to server or server to client were attempted to decrypt. Through signaling messages, types of Codecs were also found. However, with recent changes in security architecture of WhatsApp protocol (i.e. end-to-end encryption), results of this paper needs re-evaluation.

Viber is known for its obscurity of communication protocol. The fundamental work on Viber security analysis was provided in (Appelman, Bosma, & Veerman, 2011). Since then the security architecture of Viber has gone through number of phases and the latest version of Viber is providing end-to-end encryption for voice and video calls. Similarly, chat messages and file sharing services are also encrypted. A recent comprehensive work on Viber traffic analysis was presented in (Marik et al., 2015) which discussed observation-based analysis of Viber communication protocol between servers and clients, pattern classification depending upon payloads and vulnerability assessment. The survey of this paper was clearly distributed between two distinct periods of Viber until 2014, when a number of security breaches existed in the design and Viber after April 2014 when client-server communication was encrypted. The applicability of analysis of this work is no more valid for Viber 6.0 (released around March/April 2016) and beyond as the current design is based on Openwhisper security architecture which ensures end-to-end encryption.

The analysis carried out in our work covers upto latest version of Viber 6.2.2 and all results were verified for both android and iOS platforms. Behaviour of traffic of Viber was extensively studied and signatures of Viber were identified based on observed patterns in traffic. A large number of events of Viber communication were stimulated to draw conclusions about the traffic classification. The reliability and accuracy of traffic classification was increased by mixing the techniques of port based identification, tracking the fixed byte patterns as identifiers and monitoring the state flows within data and control traffic. Through necessary screen shots and process flow charts, detection of Viber traffic over the network and its further classification into voice and video chats, file sharing and text messaging is demonstrated in this work.

3. VISUALIZATION OF VIBER TRAFFIC

This section elaborates the methodology of interception of Viber traffic and its further filtering to accurately identify the Viber voice/video communications and chat conversations. To do so, a large number of traffic samples were collected by using different mobile devices running commonly used operating systems (e.g. Android/iOS). The accurate detection of Viber traffic over the network along with all services was achieved through deep analysis.

The security architecture of Viber is no more totally opaque and even the latest updates of security design are available on Viber website (Rakuten, 1997 (accessed 30-August-2016)). Now we summarize the contents of Viber security overview here. The most recent changes in the security architecture of Viber started with Viber 6.0, after which all of Viber's services were secured. The end-to-end encryption is provided for voice and video calls, one-on-one chats and group messages, secondary devices (other devices running Viber with the same account) and media sharing. The core of security engine is Salsa 20 stream cipher which is used for payload encryption. The secure ses-

sions are established using Elliptic-Curve Diffie-Hellman key-exchange algorithm and HMAC-SHA256 for authentication. The storage of encryption keys is only maintained on the client smartphones and not even the Viber servers have access to them.

Driving the motivation from Open Whisper Systems Signal application; Viber's security architecture is based on the double ratchet protocol which provides forward and backward secrecy. If a key of any session is compromised, past and future messages cannot be decrypted. A secure session is established between the two users once and then unlimited number of messages can be exchanged in either direction. Similarly, for secure call (voice and video) sessions, session keys are established which are then used to convert RTP streams to SRTP via Salsa encryption algorithm. The file sharing is also end-to-end secure.

For group messaging, all members of the group share a secret common key which is generated by group creator and shared with other members of the group through secure sessions. As per the claims of Viber designers, not even Viber has any visibility to these group keys. Additionally, mechanism of identity authentication is incorporated in Viber through which string of 48 decimal characters is matched by caller and the callee during a live call. This authentication procedure protects the users form threat of any man-in-the-middle possibility. The only known limitation of Viber till date is related to iOS pictures and video sharing service which is not end-to-end encrypted. However, the designers of Viber security commit to patch this vulnerability in near future.

3.1 Setup For Network Traffic Collection

This section explains the layout of our setup to collect Viber traffic over the network for our analysis. As shown in Figure 1, a TP-Link wireless router was connected to the Layer 3 switch with internet connection terminated on it as well. In this scenario, TP-Link wireless router provided the internet in its vicinity. A mirroring port of the switch was configured to collect the entire traffic of the port to which the TP-Link router was connected. The data of mirroring port was fed to our proprietary setup to analyze the traffic of the mobile.

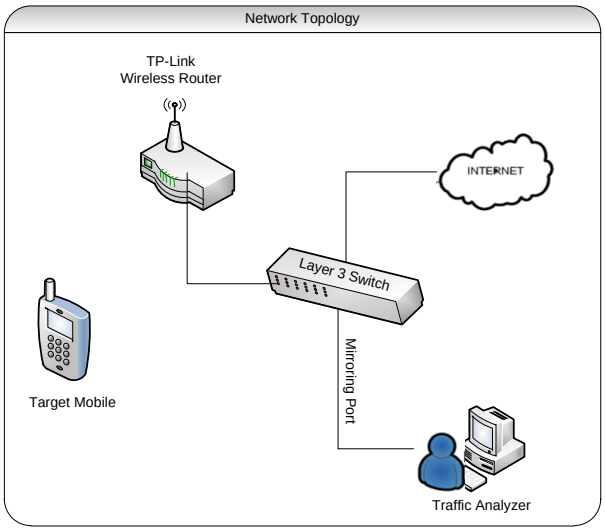

Figure 1. Network traffic collection

On successful configuration of layout of capturing and mirroring the traffic, the target mobile was connected to TP-Link router and we started getting the captured packets on the traffic analyzer. Any traffic analyzer like Wireshark can be used to capture the entire traffic going in and out from the mobile device and to save as pcap-file for detailed analysis. First, we demonstrate the analysis of Viber voice/video communication and then the chat messages.

3.2 Viber Voice and Video Call

In this Section, study of Viber calls identification and complete flow of our classification methodology is discussed. It was observed that for every session of voice or voice/video call, Viber converted the RTP stream of voice/ video to securer stream of SRTP while using Salsa20 encryption algorithm. The sessions between the Viber caller to server and server to callee were all encrypted and communication with distributed IPs made the analysis further complex. However, with known and observed peculiarities of TCP and UDP flows, byte patterns and tracking their flows, successful identification of calls and their further classification was

achieved.

3.2.1 Call Detection

After the detailed analysis of thousands of traffic samples, it was found that whenever the caller initiated a voice call, the voice messages first communicated via server between the caller and the callee. During the call, the encrypted signaling messages were exchanged either on UDP or TCP to establish P2P connection between the two users. This phenomena will be demonstrated later. On getting the traffic dump as shown in Figure 2, our first task was to detect and filter out the Viber communication between the two entities of interest.

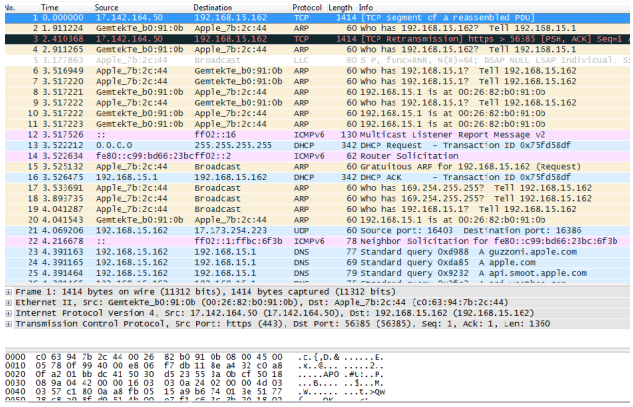

Figure 2. Unfiltered traffic

Viber usually communicates over UDP ports 7985, 7987, 5243 and 9785 for the voice calls and the same was observed over the entire period of our study. By applying the filters on these ports along with the IP address of the target mobile (i.e 192.168.15.162), we observed two distinct communication streams on port 7985 as shown in Figure 3 and on port 7987 as shown in Figure 4.

The target mobile tried to establish the connection on port 7985 and 7987 simultaneously as depicted in Figure 5 but only succeeded to establish the connection on port 7985. We would also like to note that only 4 packets were being exchanged to port 7987 of the Viber server during the entire voice session. It could be safely inferred that attempts of establishing connection on multiple server ports were made and reliable connection was achieved on one of these

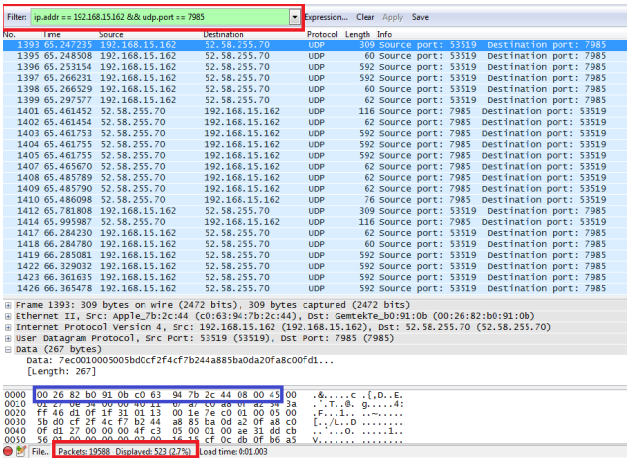

Figure 3. Traffic with target IP and server port 7985

UDP server ports.

We repeatedly observed that the caller tried to establish the P2P connection with the callee directly and logical interpretation of these attempts could be to release the load of voice/video traffic over the server and utilize the resources of individual clients. Another important observation was related to fixed port used by the caller for establishing connection with Viber server and during its continuous attempts for P2P connection with the callee as well. As shown in Figure 6, the target mobile already connected to the server while exchanging the voice messages with IP 52.58.255.70 via server, was also trying to establish the P2P connection with the callee having IP 43.245.8.10 on multiple ports including 54761, 54762, 54763 and 54764. These IP and ports of the other party were definitely sent over the encrypted communication with server (on either TCP or UDP)

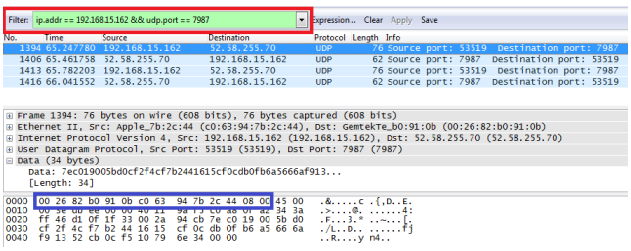

Figure 4. Traffic with target IP and server port 7987

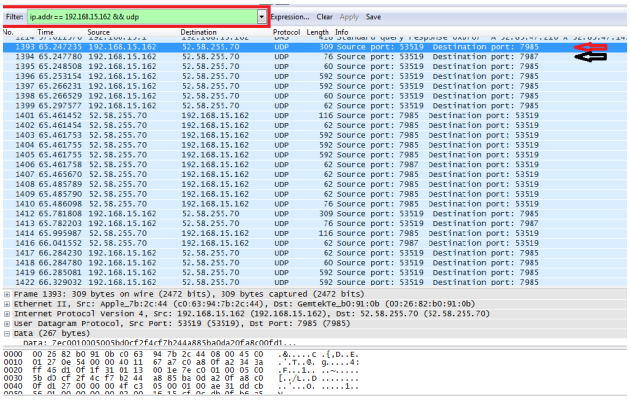

Figure 5. Connection requests from target IP to multiple UDP server ports

otherwise it was not possible for the target mobile to initiate such direct messages to the other user. Similarly , UDP port of 53519 was assigned to the caller during its connection with the Server and remained fixed during its P2P attempts.

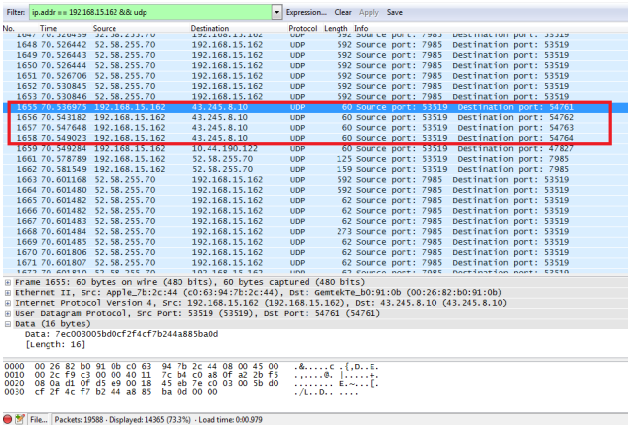

Figure 6. Multiple P2P connection requests

3.2.2 Behavior Analysis of Viber Voice/Video Call

Once the Viber call was identified and segregated from the entire traffic, the behavior analysis was performed to distinguish between the voice and video call or switch over events between the voice and video and vice-versa. It was very challenging for us to implement the efficient, reliable and accurate algorithm to differentiate between these two events specially while they are changing frequently during a single session.

We observed that the Viber operated normally at the rate of 40 to 90 UDP packets per second with different payload sizes. We focused our analysis on voice and video traffic payloads exclusively through thousands of triggered events with extensive switch over from voice to video and vice-versa. Our finding revealed that the payload size of a voice was normally greater than 18 bytes and less than 300 bytes with possibility of little variations. Similarly, packets with size greater than 750 bytes and less than 1400 bytes were seen frequently in a video call.

With slow internet connection, the video call turned into voice call immediately but few packets of UDP payload of size greater than 750 were also observed to be exchanged. We catered different corner cases as well in our algorithm to identify the event of voice or video calls correctly. To achieve accuracy of our findings, focus of our research was to identify following parameters in Viber conversations.

1. Duration of the call.

2. Correct call event (i.e. voice or video).

Table 1 shows the frequency of payload sizes of two different ranges in both the voice and video conversations of each side. The results were tested and verified on thousands of voice and video call events.

Figure 7 shows the P2P voice conversation between the caller and the callee and event of call switch over from voice to video. Before packet number 4664, the voice call was established and event of switch over from voice to video took place at packet number 4667. UDP payload size of 1116 was observed to be sent at this instance from IP 43.245.8.10 to the target mobile having IP 192.168.15.162. From here on, 30 to 50% of the packets/second having size greater than 18 bytes and less than 300 bytes and 50 to 70% of the packets/second having size greater than 750 bytes and less than 1400 bytes were sent from IP 43.245.8.10 to the target mobile. During the voice call, all packets of length greater than 18

Event	**Payload Size (PS)** $18 < PS < 300$	**Payload Size** (PS) $750 < PS < 1400$
Voice call	Yes 100%	No
Video call	Yes (30% to 50%)	Yes (50% to 70%)

Table 1. Payload sizes for Voice and Video calls

bytes and less than 300 bytes were exchanged between the two parties.

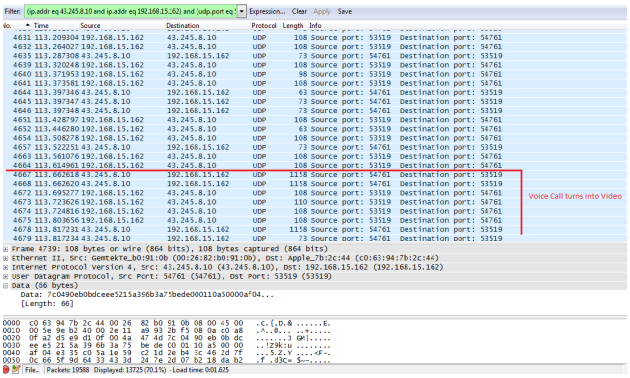

Figure 7. Voice call turns into video

3.2.3 Flow Chart for the Identification of Viber Call Events and Duration

The flow chart as shown in Figure 8 gives the implementation model of our idea to detect Viber voice and voice/video conversations accurately. The behavior analysis on massive number of traffic samples was carried out to define the discrete steps of our flow chart. The process described in this flow can serve to be main framework of developing signatures of Viber traffic even it is encrypted.

Once the incoming traffic was intercepted by the packet receiver, it sent the stream to Viber detection component to filter out Viber call traffic. This traffic was then sent to Viber Analyzer to identify the voice or video traffic. The design of Viber analyzer incorporated our all findings on voice calls, video calls and switch over between voice to video and video to voice events. The Viber analyzer module continuously extracted all IPs and their corresponding ports from the received traffic and maintained the dictionary.

Viber detection component was responsible to first decode initial session of Viber traffic by looking at the UDP ports including 7985, 7987, 5243 and 9785. When a P2P session was observed to be established, Viber detection component decoded the Viber traffic by trying to find out the hash of source IP with source Port or destination IP with destination Port in the internal dictionary of extracted IPs and ports maintained by the Viber analyzer. When the traffic arrived at Viber analyzer, it extracted client IP and client port to perform the following operations:-

1. Maintained its own dictionary of client IP and client port along with counters for different types of packets, call events, and timing markers.

2. Sent the client IP and client port to Viber detection component for P2P session identification of Viber call traffic.

   When the first packet arrived, it initially triggered the event log component to check voice or video on the basis of payload length of the packet. Now, for every single packet, the Viber analyzer examined for switch over event between voice to video or vice-versa. After studying million of packets in consonance to triggered events, fixed patterns of traffic were determined which made our detection mechanism accurate. Similarly, timing component of our model clearly identified the events duration, their start and termination instances.

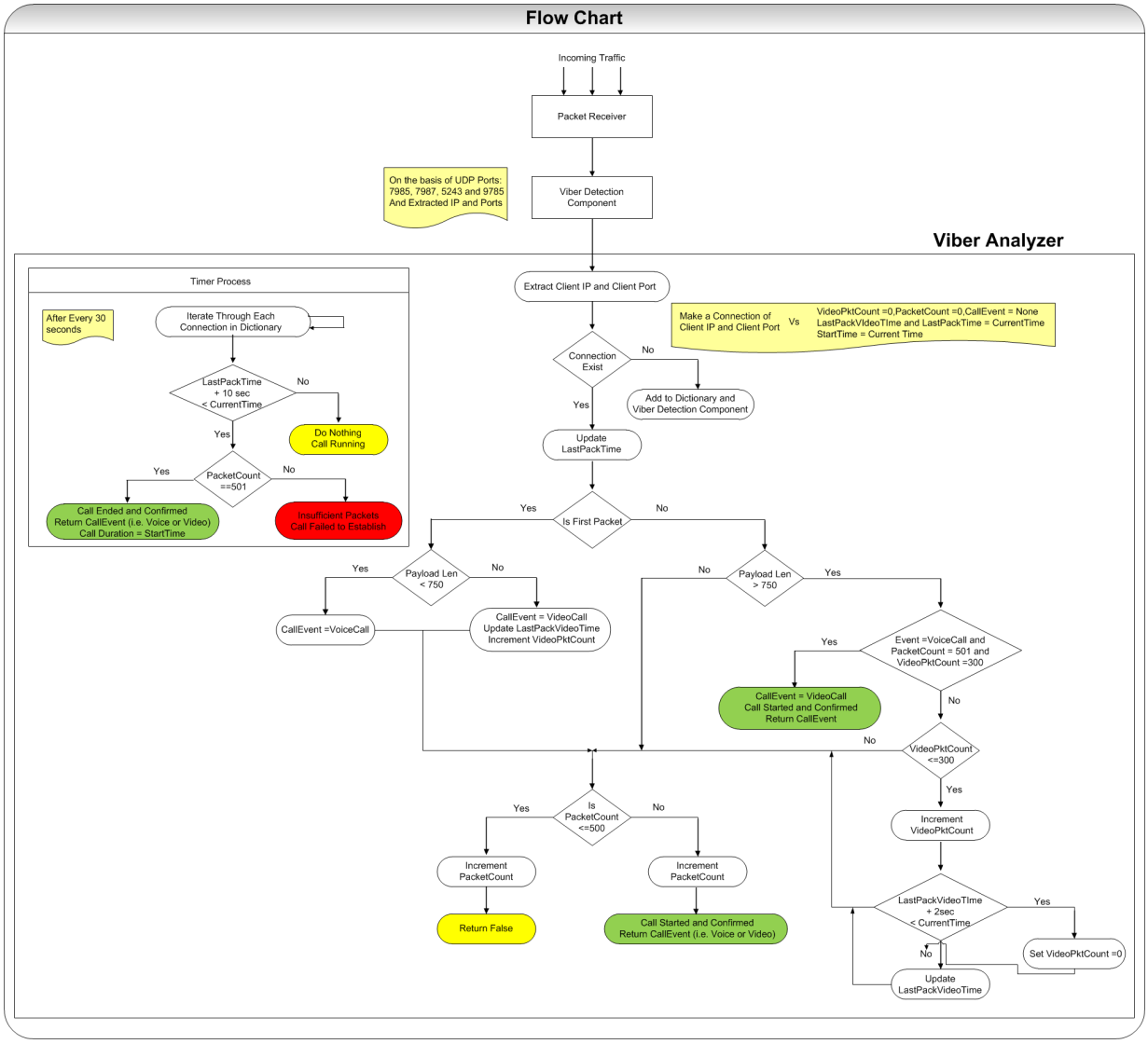

Figure 8. Viber call identification flow chart

3.3 Viber Chat Conversation Events Identification

Viber normally uses TCP ports 5242 and 4244 for providing chat services to the clients. We observed that a user always made a persistent connection with the Viber server on the above specified ports until the user signed out or the internet connection was disturbed. We defined following events of chat conversation to each of the chat participants for Viber:

(a) The user was typing a message.

(b) Message sent but not delivered to the other user (the other user was offline).

(c) Message sent and delivered but not seen by the other user (the other user was online but the message was still unread).

(d) Message sent and seen by the other user (the other user read the message).

(e) Message received but not seen by the user (the user was online but the message was still unread).

(f) Message received and seen by the user (the user read the message).

Event	TCP Payload Size	From	To	Freq
User is typing	92 bytes	client	server	variable
Message sent but not delivered	98 bytes	server	client	atomic
	84 bytes	client	server	atomic
Message sent and delivered but not seen by recipient	98 bytes	server	client	atomic
	84 bytes	client	server	atomic
	119 bytes	server	client	atomic
	64 bytes	client	server	atomic
Message Sent and seen by recipient	98 bytes	server	client	atomic
	84 bytes	client	server	atomic
	119 bytes	server	client	atomic
	64 bytes	client	server	atomic
	105 bytes	server	client	atomic
	103 bytes	client	server	atomic
Message Received but not seen by recipient	68 bytes	client	server	atomic
Message Received and seen	68 bytes	client	server	atomic
	103 bytes	client	server	atomic
	100 bytes	server	client	atomic

Table 2. Identification of chat conversation events

After conducting extensive behavior analysis of the chat conversation between the two users, we were able to identify all of these events of a particular chat conversation. For each event, a pattern of TCP packets with constant payloads was observed as mentioned in the Table 2.

Possible events of chat conversation were generated and behaviour of traffic was determined by analyzing client-server connection establishment, tracking flows of traffic, timing of exchange of fixed byte patterns, payload size and frequency of connection requests and responses. A reliable set of parameters defining the Viber chat conversation and its different events were then used to develop a tool. The developed utility was tested over the network for accuracy and reliability of identification of Viber chat messages and their event wise classification.

For each received packet, an acknowledgement packet was sent exclusively from the other side. However, the order of these acknowledgement packets in a particular event may vary. Voice chat messages, group messages, and media sharing (picture, video, and file) chats also worked in the same way and their patterns were correctly identified using the parameters outlined in Table 2.

As mentioned above, the client always made a persistent connection with the Viber server. We observed that following messages were exchanged after regular intervals to keep the server-client connection alive.

(a) Packet containing 101 bytes of TCP payload was sent from client to server.

(b) Packet containing 76 bytes of TCP payload wass sent from server to client.

Our findings on classification of chat events with respect to payload sizes and correct event identification were tested over thousands of traffic samples of Viber.

3.4 Summary of our Findings

In developing the signatures of Viber traffic and its services, we were able to:

(a) Identify traffic of Viber over the network with accuracy.

(b) Classification of voice calls, video calls and switch over between voice to video and video to voice.

(c) Identification of IPs of both parties of voice or video calls.

(d) Classification of chats including text chats, voice chats, group chats and media sharing during chats.

Besides the limitation of encrypted contents, the identification of both parties for messaging/chat service was not possible in current version of Viber which can be termed as limitation of traffic analysis observed so far; however, the same can be a dimension of future work for other researchers of community. Similarly, analysis of other messaging applications can be undertaken by forensics community based on our demonstrated methodology. It is important to mention that new security patches and updates in communication protocol of any social media app entails re-verification of previous analysis results. We consider it a continuous process both for the designers of proprietary messaging/chat applications and for forensics community.

4. CONCLUSION

In this work, we demonstrated a reliable framework of identification of secure Viber traffic over the IP network and its further classification in to voice calls, voice/video calls, chat messages (text and voice), group messages, and media sharing. Our analysis is considered to be the most recent one after the release of Viber 6.0 around March/April 2016, which provided end-to-end encryption and authentication against man-in-the-middle attacks. Our results are applicable to the latest version of Viber until 31 August 2016.

Against the opaque communication protocol of Viber, a combination of variant techniques of traffic classification was used to develop a model which correctly profiled the Viber services. We incorporated port and IP based filtering, UDP and TCP ports based flow tracking, extensive analysis of byte patterns, payload sizes and their frequency in relation to triggered events, peculiarities in server-client or client-server requests vis--vis their responses, the persistence of established sessions and their timings. We were able to map our findings on network level IP traffic successfully and verified their accuracy for android and iOS platforms.

REFERENCES

Adami, D., Callegari, C., Giordano, S., Pagano, M., & Pepe, T. (2012). Skype-hunter: A real-time system for the detection and classification of skype traffic. *International Journal of Communication Systems*, *25*(3), 386–403.

Appelman, M., Bosma, J., & Veerman, G. (2011). Viber communication security. *System and network of engineering, university of Amsterdam, Netherlands*.

Callado, A., Kamienski, C., Szabó, G., Gero, B. P., Kelner, J., Fernandes, S., & Sadok, D. (2009). A survey on internet traffic identification. *IEEE Communications Surveys & Tutorials*, *11*(3), 37–52.

Chakravarty, S., Barbera, M. V., Portokalidis, G., Polychronakis, M., & Keromytis, A. D. (2014). On the effectiveness of traffic analysis against anonymity networks using flow records. In *International conference on passive and active network measurement* (pp. 247–257).

Chakravarty, S., Stavrou, A., & Keromytis, A. D. (2010). Traffic analysis against low-latency anonymity networks using available bandwidth estimation. In *European symposium on research in computer security* (pp. 249–267).

Chen, A., Jin, Y., Cao, J., & Li, L. E. (2010). Tracking long duration flows in network traffic. In *Infocom, 2010 proceedings ieee* (pp. 1–5).

Coull, S. E., & Dyer, K. P. (2014). Traffic analysis of encrypted messaging services: Apple imessage and beyond. *ACM SIGCOMM Computer Communication Review*, *44*(5), 5–11.

Dainotti, A., Pescape, A., & Claffy, K. C. (2012). Issues and future directions in traffic classification. *IEEE network*, *26*(1), 35–40.

Gilad, Y., & Herzberg, A. (2012). Spying in the dark: Tcp and tor traffic analysis. In *International symposium on privacy enhancing technologies symposium* (pp. 100–119).

Karpisek, F., Baggili, I., & Breitinger, F. (2015). Whatsapp network forensics: Decrypting and understanding the whatsapp call signaling messages. *Digital Investigation*, *15*, 110–118.

Marik, R., Bezpalec, P., Kucerak, J., & Kencl, L. (2015). Revealing viber communication patterns to assess protocol vulnerability. In *2015 international conference on computing and network communications (coconet)* (pp. 496–504).

Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, *10*(4), 56–76.

Rakuten, I. (1997 (accessed 30-August-2016)). *Viber Encryption Overview.* `http://www.viber.com/en/security-overview`.

Rakuten, I. (1997 (accessed 9-November-2016)). *Viber: About.* `http://www.viber.com/en/about`.

Velan, P., Čermák, M., Čeleda, P., & Drašar, M. (2015). A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management*, *25*(5), 355–374.

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Digital Investigation*, *14*, S77–S84.

Yuan, Z., Du, C., Chen, X., Wang, D., & Xue, Y. (2014). Skytracer: Towards fine-grained identification for skype traffic via sequence signatures. In

Computing, networking and communications (icnc), 2014 international conference on (pp. 1–5).

Zhang, F., He, W., Liu, X., & Bridges, P. G. (2011). Inferring users' online activities through traffic analysis. In *Proceedings of the fourth acm conference on wireless network security* (pp. 59–70).

Zhang, J., Chen, C., Xiang, Y., Zhou, W., & Vasilakos, A. V. (2013). An effective network traffic classification method with unknown flow detection. *IEEE Transactions on Network and Service Management*, *10*(2), 133–147.

