Electron Commer Res (2016) 16:73–111
DOI 10.1007/s10660-015-9208-1

Android mobile VoIP apps: a survey and examination of their security and privacy

Abdullah Azfar[1] · Kim-Kwang Raymond Choo[1] · Lin Liu[2]

Published online: 21 November 2015

Abstract Voice over Internet Protocol (VoIP) has become increasingly popular among individuals and business organisations, with millions of users communicating using VoIP applications (apps) on their smart mobile devices. Since Android is one of the most popular mobile platforms, this research focuses on Android devices. In this paper we survey the research that examines the security and privacy of mVoIP published in English from January 2009 to January 2014. We also examine the ten most popular free mVoIP apps for Android devices, and analyse the communications to determine whether the voice and text communications using these mVoIP apps are encrypted. The results indicate that most of the apps encrypt text communications, but voice communications may not have been encrypted in Fring, ICQ, Tango, Viber, Vonage, WeChat and Yahoo. The findings described in this paper contribute to an in-depth understanding of the potential privacy risks inherent in the communications using these apps, a previously understudied app category. Six potential research topics are also outlined.

Electronic supplementary material The online version of this article (doi:10.1007/s10660-015-9208-1) contains supplementary material, which is available to authorized users.

✉ Abdullah Azfar
abdullah.azfar@mymail.unisa.edu.au

Kim-Kwang Raymond Choo
raymond.choo@unisa.edu.au

Lin Liu
lin.liu@unisa.edu.au

[1] Information Assurance Research Group, University of South Australia, Adelaide, Australia

[2] School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia

Keywords Android applications · Voice over Internet Protocol (VoIP) · Mobile VoIP (mVoIP) applications · Security and privacy of mobile VoIP apps

1 Introduction

In the past years, there has been a noted convergence between mobile telephone networks and the Internet because of the latter's capability to deliver enhanced social and mobile experiences. The Voice over Internet Protocol (VoIP) market is an example of a dynamic market with a steady increase in the number of service providers and Internet service providers offer VoIP services, as a part of a bundled Internet package, which do not require a fixed line telephone to make local and international calls.

VoIP has been viewed as a positive driver for e-business models, which can potentially increase relational capital [7]. An example is seen in a study by the Australian Government Department of Broadband, Communications and the Digital Economy [2], which found that the number of Australian 'adults using voice over internet protocol (VoIP) rose by nearly 21 % in the year to June 2012, to 4.3 million'. This is, perhaps, unsurprising as VoIP provides voice and video communications, which are cost effective, and in some cases, free on both personal computers and mobile devices [e.g. using mobile VoIP (mVoIP) applications (apps) to make an app-to-app call]. Overall, VoIP has contributed to e-commerce growth both by reducing the communication cost and by providing low-cost technological infrastructure, cheaper customer service alternatives and economic electronic transactions with suppliers. According to a market research report by Infonetics Research, the number of mVoIP users increased by more than 550 % in 2012, to over 640 million, and mVoIP and voice over Long Term Evolution services are expected to become a US$16 billion business by 2017 [25].

The increasingly popularity of smart mobile devices has resulted in a surge in the number of mVoIP app users for both personal and business purposes [10]. However, like most forms of electronic communications, mVoIP communications can be intercepted by malicious actors. Examples include the compromisation of a client machine such as a mobile device using malware with the intention of intercepting the voice or video communication before it is encrypted by the mVoIP app [47], and interception of information by government agencies authorised by a wiretap warrant[1] [31]. Despite this, the security of communications using mVoIP apps appears to be an understudied area. To date, there are relatively few publications on the topic as demonstrated in our survey (see Sect. 2).

In this paper, we review the research on mVoIP security and privacy issues that has been published in the last 5 years (i.e. January 2009 to January 2014), and examine ten most popular free mVoIP apps for Android devices to determine whether app-to-app communication (both voice and text) using specific apps (e.g.

[1] Although the PRISM program by National Security Agency reportedly allows the U.S. intelligence community to gain access from nine Internet companies to a wide range of digital information [34], including VoIP and mVoIP communications, such capabilities are not typically available to other non-state actors or most non-U.S. state actors.

Viber app to Viber app) are encrypted. Three different app-to-app communication channel combinations are considered: (a) mobile data network to mobile data network (m2m), (b) mobile data network to WiFi network (m2w), and (c) WiFi network to mobile data network (w2m); as WiFi network to WiFi network (w2w) where both end users that use WiFi networks were considered in our earlier work [4]. The communications are captured locally in the devices and no malicious software (malware) is used in this process. We then analyse the captured text and voice communications using the histograms and the entropy of the captured communication sessions.

We regard the contributions of this paper to be two-fold:

(1) Identification of research trends on the topics of mVoIP security and privacy since 2010, based on a comprehensive survey of a previously understudied app category; and
(2) Providing mVoIP users an in-depth understanding of the potential privacy risks of using the apps examined in this paper, when they are used for text and voice communications.

The rest of the paper is organised as follows: In Sect. 2, we present a survey of the research on the security and privacy of mVoIP published in the last 5 years. Brief descriptions of the ten popular mVoIP apps are presented in Sect. 3. The experiment setup, methods for analysis, and the experiment processes are outlined in Sect. 4. In the next three sections, we present our experimental results for the three different app-to-app communication combinations m2m (Sect. 5), m2w (Sect. 6), and w2m (Sect. 7). In Sect. 8, we discuss the findings. The last section concludes the paper, and outlines six potential research topics.

2 mVoIP security and privacy: a survey

As illustrated in Fig. 1, VoIP security is a very popular research topic during 2005–2008, and mVoIP is a more recent research trend—emerging as a salient area of inquiry by researchers (e.g.in the areas of security and privacy) [29]. This is not surprising, as this communication medium is only adopted by both individual and

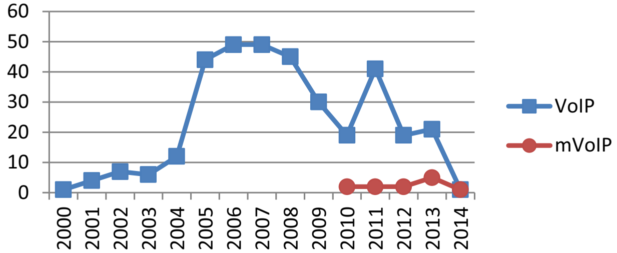


Fig. 1 Research trends on VoIP and mVoIP security and privacy since 2000

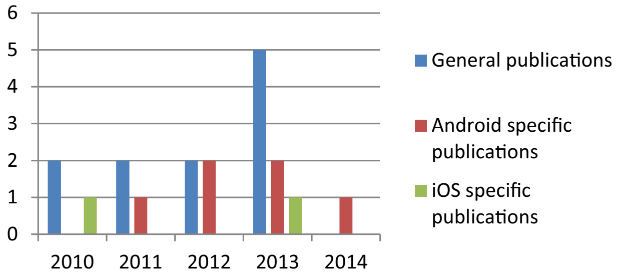


Fig. 2 Publications relating to mVoIP security and privacy from calendar year 2010 to 2014 (a total of 12 publications were located)

corporate mobile users when smart mobile devices become a popular alternative to computers. The survey also revealed that mVoIP security and privacy research is generally dependent on the popularity of the platform/operating system (OS),—see Fig. 2. The interested reader is referred to Online Resource 1 for the full survey of the research on mVoIP security and privacy published from January 2009 to January 2014.

3 Ten popular mVoIP apps

As evidenced from the survey in the earlier section, the security and privacy of mVoIP is an emerging but under-studied research topic. We aim to contribute to the literature gap, by studying ten most popular free mVoIP apps. In this section, we give an overview of these apps that support text, voice and video communications, namely Skype, Google Hangout (recently replaced Google Talk), ICQ, Viber, Nimbuzz, Yahoo, Fring, Vonage, WeChat and Tango. At the time of research, we use the latest version of the apps in our study. The details of experiment setup and analysis will be provided in Sect. 4 and the findings will be presented in Sect. 5.

Skype is one of the most widely used mVoIP apps with an estimated 40 % market share in 2012 [25]. Skype uses its own proprietary secure VoIP communication protocol [48]. All the packets of Skype communication are encrypted with the 256-bit Advanced Encryption Standard (AES) [3]. Skype servers certify user public keys using either 1536 or 2048-bit RSA certificates [15]. Since it is trivial to determine a target's Skype ID, an attacker can therefore communicate with the target over Skype to determine his/her IP address, even if the target is behind a network address translation (NAT) server [6]. Once the IP address of the user is located, the user's mobility can then be monitored.

Google Talk uses Extensible Messaging and Presence Protocol (XMPP) [28], which provides voice communication services through an extension named Jingle [30]. The Jabber stream is not encrypted in Google Talk [23, 26]. Google Talk also uses its own authentication mechanism. Google Hangout replaced Google Talk in 2013. Google Hangout encrypts the text communications over an HTTPS connection with 128-bit encryption, using TLS 1.2, and voice communications are encrypted using 128-bit AES encryption [21]. Unlike Google Talk, Google Hangout uses its own proprietary protocol [36] and requires a valid Gmail account to login. Viber, WeChat, Fring, Tango and Vonage, on the other hand, use the number of the mobile handset (e.g. +61 400 123456789) that the mVoIP app is installed on as the authentication mechanism and user ID.

ICQ is another popular mVoIP app, which uses proprietary Open System for Communication in Realtime (OSCAR) messaging protocol. ICQ is available for Windows, Apple iOS, Blackberry, Symbian and Android platforms. Although the company's documentation suggests that ICQ does not provide encryption [24], our findings indicated that text communications are encrypted (see Table 3 in Sect. 8).

Although Viber is relatively new, it has gained popularity among users. Viber does not need a separate login other than a user name, either using WiFi or mobile data network to send or receive voice calls and messages [44]. Viber provides encrypted text messaging services [43] and scrambles voice data [1]. Viber uses its own proprietary protocol. In 2013, a bug was discovered in Viber where the lock screens of smart phones can be bypassed to send voice calls and messages [5].

Yahoo messenger uses its own proprietary protocol to provide instant messaging, photo sharing, PC-to-PC calls, mail alerts, games and other features [51]. A Yahoo voice server was compromised in 2012, which resulted in the theft of 453,491 Yahoo email messages and passwords [38].

Nimbuzz is a communication platform that provides voice and video call services over the Internet [33]. Nimbuzz connects with popular instant messaging and social network sites such as Facebook, Google Talk and Yahoo messenger. Nimbuzz uses XMPP as its primary protocol [45].

Similar to Nimbuzz is another communication platform Fring [17]. Fring is a P2P VoIP service provider, which uses Dynamic Video Quality (DVQ) technology for video calls. Tango [42] uses its own protocol and provides free VoIP calling services between Tango users.

Vonage provides a VoIP application—Vonage Mobile [46]. WeChat [49] is another popular VoIP application developed by the Chinese company, Tencent (the same company that developed Tencent QQ, reportedly one of the widest used instant messaging application in China).

We used the most recent version of the apps as of 17 September 2013 in the experiments, as summarised in Table 1. The majority of the mVoIP apps run on Android, iOS, Windows, Blackberry and Symbian platforms; and a mobile phone number (also known as a cell phone number in the United States) is generally used as the user ID.

4 Experiments

4.1 Experiment setup

In our experiments, we used two LG Google Nexus 4 Android phones with Android version 4.2.2. Android application Shark for Root was used to capture network

Table 1 Supported platforms and authentication methods of the mVoIP apps

mVoIP apps	Supported mobile platforms					Version used in our experiments	Authentication method (and user ID)
	Android	iOS	Windows	Blackberry	Symbian		
Skype	✓	✓	✓	✓	✓	4.0.0.26576	User name and password
Google Hangout	✓	✓				1.1.2.778356	A valid Gmail account
ICQ	✓	✓	✓	✓	✓	4.0.8	User name (a valid Email account) and password
Yahoo	✓	✓	✓	✓	✓	1.8.3.13903	A valid Yahoo account
Nimbuzz	✓	✓	✓	✓	✓	2.6.0	User name and password
Viber	✓	✓	✓	✓	✓	3.1.1	
WeChat	✓	✓	✓	✓	✓	5.0.1	
Fring	✓	✓			✓	4.4.2.1.4–6	Mobile phone number (e.g. +61 400 123 456)
Tango	✓	✓	✓			3.1.58939	
Vonage	✓	✓				2.2.2	

Table 2 Song details for sample 1 and sample 2

	Songs	Artist	Start time	End time	Duration
Sample 1	When you say nothing at all	Ronan Keating	00:00	04:13	10:03
	Stop	Spice Girls	00:00	03:12	
	Another day in paradise	Phil Collins	00:00	02:35	
Sample 2	Last Christmas	George Michael	00:00	04:15	10:04
	I want it that way	Backstreet Boys	00:00	03:39	
	Picture of you	Boyzone	00:00	02:10	

traffic in pcap format. The mVoIP apps were run on both phones one at a time. Voice and text messages were captured separately.

For each of the ten apps, we captured voice data in both directions for 10 min. This was done to ensure the reliability of the experiment, and the same set of songs (see Table 2) were used in our earlier work [4]. The entire process was undertaken for the three different combinations of app-to-app communication, namely (a) mobile data network to mobile data network (m2m)—see Sect. 5, (b) mobile data network to WiFi network (m2w)—see Sect. 6, and (c) WiFi network to mobile data network (w2m)—see Sect. 7.

We then sent a series of text messages using the ten apps respectively and captured the communications to analyse the captured text communications for the above three app-to-app communication combinations. To ensure that there was no other traffic, all other apps that could generate Internet traffic were turned off.

4.2 Methods for analysis

It is relatively straightforward to determine whether text messages sent using text messaging apps are encrypted, by analysing the captured packets. However, determining whether the captured voice communications are encrypted is less straightforward due to a number of reasons, such as:

(i) Codecs are used to encode and compress voice signals into a lower entropy signal. Some codecs use irreversible compression techniques, such as lossy compression. Due to the encoding and compression applied by the codecs, it is hard to determine whether the captured packets are encrypted.

(ii) To decode the captured voice data, we need to use the right decoder. In cases such as open source VoIP apps based on Session Initiation Protocol (SIP), the payload type of the captured data indicates the codec used in the encoding. However in the case of proprietary VoIP apps (e.g. Skype), there is no indication of the payload type in the captured packets. The captured TCP or UDP communication will only indicate unassigned payload types.

We applied two statistical methods, namely Histogram and Entropy analysis, to determine whether the voice communications are encrypted.

4.2.1 Histogram analysis

Histogram analysis is one of the commonly used graphical approach to examine the distribution of data. For example, histogram analysis was used by Ghaemmaghami et al. [18] to detect voice activities on noisy speech, and entropy analysis has been used by researchers such as Dorfinger et al. [16] for detecting encrypted traffic and Gomes et al. [20] to identify and classify P2P (Peer to Peer) VoIP sessions.

The output of a secure encryption algorithm is probabilistic—i.e. encryption of the same message twice is unlikely to result in the same ciphertext, and knowing the encryption of a message may not help us recognise another encryption of the same message. In other words, a secure encryption algorithm will produce a message that is randomly distributed [12, 19], and as Guo et al. [22] demonstrated in their study, 'encrypted voice is randomly distributed'. A secure encryption algorithm generates a data stream with uniformly distributed codewords designed to resist statistical attacks [27].

Therefore, if the communications are encrypted, the number of occurrences of each byte in the captured pcap files would also be evenly distributed; otherwise, the number of occurrences of each byte in the captured pcap files will be scattered and clustered. Wright et al. [50] used this approach to identify the language used in a VoIP conversation. Pcap Histogram [35] is one of several tools that can be used to analyse encrypted payload based on their statistical distribution [8]. This approach was chosen solely for its simplicity in determining whether the voice communication is encrypted (or not). We acknowledge that there are likely more advanced signal processing approaches, but this was outside the scope of our research.

4.2.2 Entropy analysis

The entropy of the payloads of the captured packets was calculated using Shannon entropy, which measures the uncertainty associated with a random variable [39]. Given a random variable X with N possible values $\{x_1, x_2, \ldots, x_N\}$, its entropy can be calculated as:

$$\mathrm{H(X)} = -\sum_{\mathrm{i=0}}^{\mathrm{N-1}} \mathrm{p_i} \log_2 \mathrm{p_i}, \quad \text{where} \quad \mathrm{p_i} = \mathrm{P(X = x_i)}$$

The minimum average number of bits per character is:

$$\text{numCharacters} = \text{Upper bound of } \mathrm{H(X)}$$

English language has a low entropy of 2.3 bits per character on average due to its predictable nature. However, for encrypted packets, the bits are evenly distributed and the entropy value increases (greater than 5 bits per character on average).

The lack of encryption results in frequent changes in the entropy with high and low peaks, while encryption mechanism distributes the characters evenly. Therefore, the entropy of encrypted voice data is high and the entropy distribution is even (i.e. no sudden changes of high or low peaks). This can be used as the indicator to identify encrypted voice data. In our analysis, the entropy of the captured packets is calculated by the Shannon's entropy measurement tool, pyNetEntropy [37].

4.3 Experiment process

We played the same set of English language songs (sample 1 as on Table 2; and sample 2 as on Table 2) on the phones for all the ten apps in order to maintain consistency, using the following process (also see Fig. 3).

- *Step 1* Root the Nexus 4 mobile phones.
- *Step 2* Install Shark for Root app in on the phone from which pcap files will be captured.

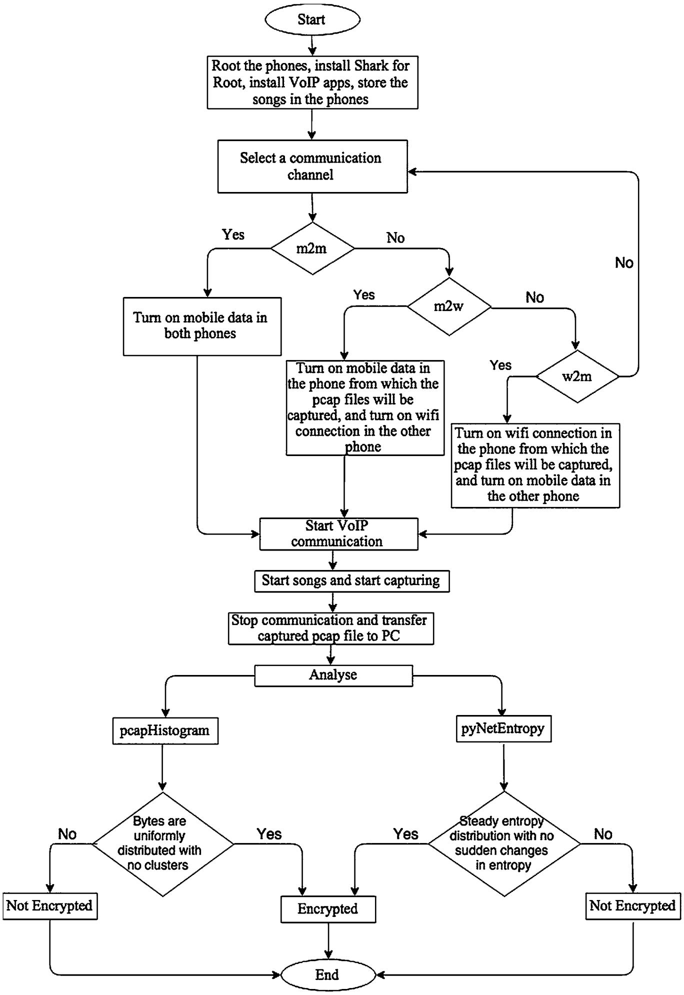

Start
Root the phones, install Shark for Root, install VoIP apps, store the songs in the phones
Select a communication channel
m2m
Yes
No
Turn on mobile data in both phones
m2w
Yes
No
Turn on mobile data in the phone from which the pcap files will be captured, and turn on wifi connection in the other phone
w2m
Yes
No
Turn on wifi connection in the phone from which the pcap files will be captured, and turn on mobile data in the other phone
Start VoIP communication
Start songs and start capturing
Stop communication and transfer captured pcap file to PC
Analyse
pcapHistogram
pyNetEntropy
Bytes are uniformly distributed with no clusters
No
Yes
Steady entropy distribution with no sudden changes in entropy
Yes
No
Not Encrypted
Encrypted
Not Encrypted
End

Fig. 3 Flowchart of the experiment process

- *Step 3* Install the VoIP apps (e.g. Skype, Viber) in both phones.
- *Step 4* Store the songs to be used under in the experiment in the phones.
- *Step 5* Select a communication channel.
  - For m2m communication, mobile data will be switched on in both phones.
  - For m2w communication, mobile data will be switched on in the phone from which the pcap files will be captured, and WiFi connection will be switched on in the other phone.
  - For w2m communication, WiFi connection will be switched on in the phone from which the pcap files will be captured, and mobile data will be switched on in the other phone.
- *Step 6* Start communication between the two phones over using the VoIP app (e.g. Skype) and play the songs. Keep surrounding noise level to a minimum, and it is highly recommended to perform this experiment in a quiet room. Start capturing the pcap files by turning on the capture mode in Shark for Root.
- *Step 7* After playing the first set of songs for 10 min, stop capturing pcap files, turn off the communication over VoIP app, and transfer the captured pcap file to a desktop PC or laptop through cable connection.
- *Step 8* Repeat steps 6 and 7 for the same app by playing the second set of songs.
- *Step 9* Repeat steps 6, 7 and to 8 for the other remaining VoIP apps.
- *Step 10* From the captured pcap files, filter only the RTP streams using Wireshark.
- *Step 11* Prepare a desktop PC or laptop with using Ubuntu or any other Linux distribution. Install the dependencies needed for executing the pcap Histogram and pyNet Entropy scripts.
- *Step 12* Analyse the pcap files using the pcap Histogram tool. Based on the histogram charts of the analysis from the pcap Histogram tool, the communication will be classified as either encrypted or not encrypted based on the following criteria:
  - If the bytes are uniformly distributed with no clusters observed (i.e. the number of occurrences of each byte is approximately similar) in the pcap file, then the communication is determined to be encrypted.
  - If there is at least one region in the histogram chart where a cluster of bytes is observed (i.e. the number of occurrences for the bytes are not similar to the other regions of the chart), then the communication is determined not to be encrypted.
- *Step 13* Analyse the pcap files using the pyNet entropy script. Based on the entropy distribution charts of the analysis from the pyNet Entropy script, the communication will be classified as either encrypted or not encrypted based on the following criteria:
  - If the entropy distribution is even (i.e. steady entropy distribution with no sudden changes in entropy) with a difference of only within 1 bit per

character throughout the communication, then the communication is determined to be encrypted.

- If the entropy distribution changes throughout the communication period (i.e. not showing a steady and even distribution of entropy) with high and low peaks with more than 1 bit per character fluctuation, then the communication is determined not to be encrypted.

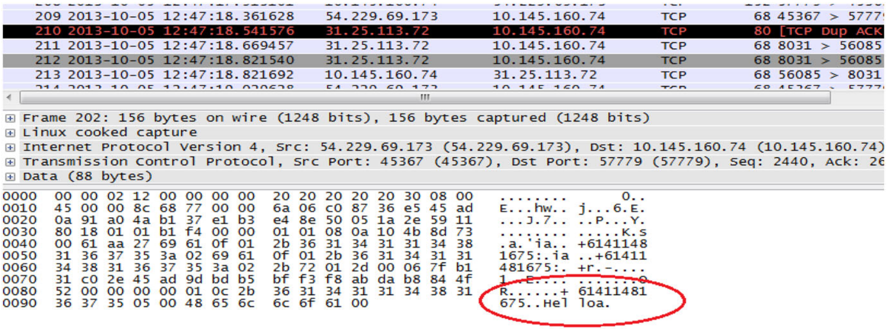
5 Findings from mobile data network to mobile data network (m2m) communications

5.1 Text data analysis

After analysing the pcap files containing text messages (captured locally in the devices), we found that most of the mVoIP apps provide encrypted communications, with the exceptions of Fring, Vonage and Yahoo messenger. For Fring and Vonage, the mobile phone number was also visible (see Figs. 4, 5). It is interesting to note that the plaintext data was not visible in w2w communication for Fring and Vonage [4], but it was clearly visible for m2m communication.

For Yahoo, we determined that outgoing text communications were not encrypted whilst incoming text communications were encrypted. In other words, text messages captured from the sender's device were found to be in plaintext, and text messages received by the sender's device were found to be encrypted. This indicates that text communication sent by Yahoo messenger (client) to Yahoo messenger server is unencrypted, but the text communication sent by Yahoo messenger server to the client is encrypted. A snapshot of the captured plaintext message is shown in Fig. 6, and the plaintext "How r u" is marked with a circle.

For Tango, the mobile phone number of the sender was in plaintext, although the messages were not readable. Analysis of the captured text messages from the remaining six mVoIP apps—Skype, Google Hangout, ICQ, Viber, Nimbuzz and WeChat—did not reveal any plaintext data or provide any clue about the sender or receiver.

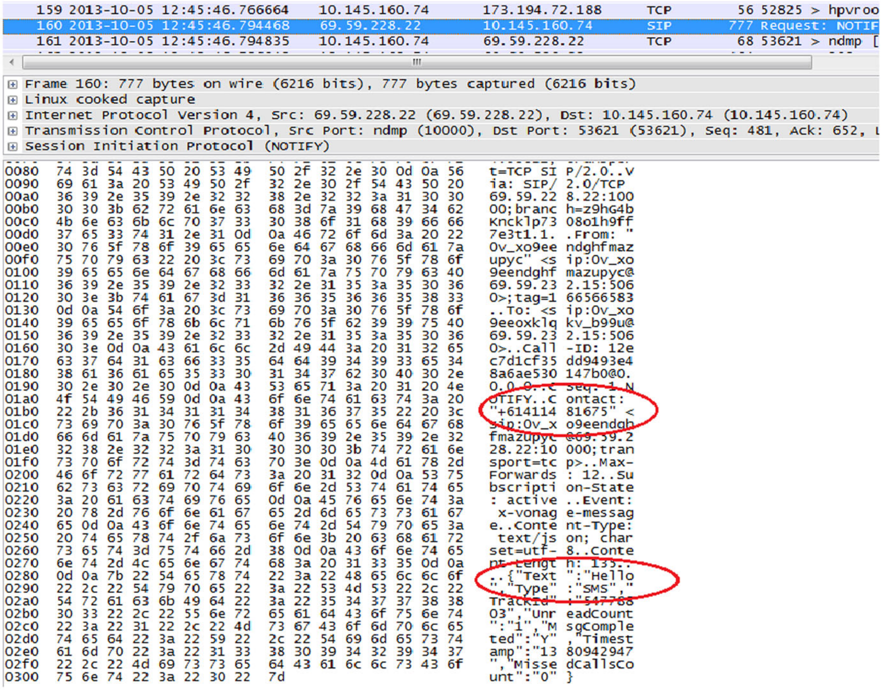


```
209 2013-10-05 12:47:18.361628   54.229.69.173    10.145.160.74    TCP    68 45367 > 5777
210 2013-10-05 12:47:18.541576   31.25.113.72     10.145.160.74    TCP    80 [TCP Dup ACK
211 2013-10-05 12:47:18.669457   31.25.113.72     10.145.160.74    TCP    68 8031 > 56085
212 2013-10-05 12:47:18.821540   31.25.113.72     10.145.160.74    TCP    68 8031 > 56085
213 2013-10-05 12:47:18.821692   10.145.160.74    31.25.113.72     TCP    68 56085 > 8031

⊞ Frame 202: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 54.229.69.173 (54.229.69.173), Dst: 10.145.160.74 (10.145.160.74)
⊞ Transmission Control Protocol, Src Port: 45367 (45367), Dst Port: 57779 (57779), Seq: 2440, Ack: 26
⊞ Data (88 bytes)

0000  00 00 02 12 00 00 00 00  20 20 20 20 20 30 08 00   ........      0..
0010  45 00 00 8c 68 77 00 00  6a 06 c0 87 36 e5 45 ad   E...hw.. j...6.E.
0020  0a 91 a0 4a b1 37 e1 b3  e4 8e 50 05 1a 2e 59 11   ...J.7.. ..P...Y.
0030  80 18 01 01 b1 f4 00 00  01 01 08 0a 10 4b 8d 73   ........ .....K.s
0040  00 61 aa 27 69 61 0f 01  2b 36 31 34 31 31 34 38   .a.'ia.. +6141148
0050  31 36 37 35 3a 02 69 61  0f 01 2b 36 31 34 31 31   1675:.ia ..+61411
0060  34 38 31 36 37 35 3a 02  2b 72 01 2d 00 06 7f b1   481675:. +r.-....
0070  31 c0 2e 45 ad 9d bd b5  bf f3 f8 ab da b8 84 4f   1..E.... .......O
0080  52 00 00 00 00 01 0c 2b  36 31 34 31 31 34 38 31   R......+ 61411481
0090  36 37 35 05 00 48 65 6c  6c 6f 61 00              675..Hel loa.
```

Fig. 4 Plain text mobile number in Fring text message



```
159 2013-10-05 12:45:46.766664   10.145.160.74   173.194.72.188   TCP     56 52825 > hpvroo
160 2013-10-05 12:45:46.794468   69.59.228.22    10.145.160.74    SIP    777 Request: NOTIF
161 2013-10-05 12:45:46.794835   10.145.160.74   69.59.228.22     TCP     68 53621 > ndmp [

⊞ Frame 160: 777 bytes on wire (6216 bits), 777 bytes captured (6216 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 69.59.228.22 (69.59.228.22), Dst: 10.145.160.74 (10.145.160.74)
⊞ Transmission Control Protocol, Src Port: ndmp (10000), Dst Port: 53621 (53621), Seq: 481, Ack: 652, L
⊞ Session Initiation Protocol (NOTIFY)

0080  74 3d 54 43 50 20 53 49  50 2f 32 2e 30 0d 0a 56   t=TCP SI P/2.0..V
0090  69 61 3a 20 53 49 50 2f  32 2e 30 2f 54 43 50 20   ia: SIP/ 2.0/TCP
00a0  36 39 2e 35 39 2e 32 32  38 2e 32 32 3a 31 30 30   69.59.22 8.22:100
00b0  30 30 3b 62 72 61 6e 63  68 3d 7a 39 68 47 34 62   00;branc h=z9hG4b
00c0  4b 6e 63 6b 6c 70 37 33  30 38 6f 31 68 39 66 66   Kncklp73 08o1h9ff
00d0  37 65 33 74 31 2e 31 0d  0a 46 72 6f 6d 3a 20 22   7e3t1.1. .From: "
00e0  30 76 5f 78 6f 39 65 65  6e 64 67 68 66 6d 61 7a   0v_xo9ee ndghfmaz
00f0  75 70 79 63 22 20 3c 73  69 70 3a 30 76 5f 78 6f   upyc" <s ip:0v_xo
0100  39 65 65 6e 64 67 68 66  6d 61 7a 75 70 79 63 40   9eendghf mazupyc@
0110  36 39 2e 35 39 2e 32 33  32 2e 31 35 3a 35 30 36   69.59.23 2.15:506
0120  30 3e 3b 74 61 67 3d 31  36 36 35 36 36 35 38 33   0>;tag=1 66566583
0130  0d 0a 54 6f 3a 20 3c 73  69 70 3a 30 76 5f 78 6f   ..To: <s ip:0v_xo
0140  39 65 65 6f 78 6b 6c 71  6b 76 5f 62 39 39 75 40   9eeoxklq kv_b99u@
0150  36 39 2e 35 39 2e 32 33  32 2e 31 35 3a 35 30 36   69.59.23 2.15:506
0160  30 3e 0d 0a 43 61 6c 6c  2d 49 44 3a 20 31 32 65   0>..Call -ID: 12e
0170  63 37 64 31 63 66 33 35  64 64 39 34 39 33 65 34   c7d1cf35 dd9493e4
0180  38 61 36 61 65 35 33 30  31 34 37 62 30 40 30 2e   8a6ae530 147b0@0.
0190  30 2e 30 2e 30 0d 0a 43  53 65 71 3a 20 31 20 4e   0.0.0..C Seq: 1 N
01a0  4f 54 49 46 59 0d 0a 43  6f 6e 74 61 63 74 3a 20   OTIFY..C ontact:
01b0  22 2b 36 31 34 31 31 34  38 31 36 37 35 22 20 3c   "+614114 81675" <
01c0  73 69 70 3a 30 76 5f 78  6f 39 65 65 6e 64 67 68   sip:0v_x o9eendgh
01d0  66 6d 61 7a 75 70 79 63  40 36 39 2e 35 39 2e 32   fmazupyc @69.59.2
01e0  32 38 2e 32 32 3a 31 30  30 30 30 3b 74 72 61 6e   28.22:10 000;tran
01f0  73 70 6f 72 74 3d 74 63  70 3e 0d 0a 4d 61 78 2d   sport=tc p>..Max-
0200  46 6f 72 77 61 72 64 73  3a 20 31 32 0d 0a 53 75   Forwards : 12..Su
0210  62 73 63 72 69 70 74 69  6f 6e 2d 53 74 61 74 65   bscripti on-State
0220  3a 20 61 63 74 69 76 65  0d 0a 45 76 65 6e 74 3a   : active ..Event:
0230  20 78 2d 76 6f 6e 61 67  65 2d 6d 65 73 73 61 67    x-vonag e-messag
0240  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e..Conte nt-Type:
0250  20 74 65 78 74 2f 6a 73  6f 6e 3b 20 63 68 61 72    text/js on; char
0260  73 65 74 3d 75 74 66 2d  38 0d 0a 43 6f 6e 74 65   set=utf- 8..Conte
0270  6e 74 2d 4c 65 6e 67 74  68 3a 20 31 33 35 0d 0a   nt-Lengt h: 135..
0280  0d 0a 7b 22 54 65 78 74  22 3a 22 48 65 6c 6c 6f   ..{"Text ":"Hello
0290  22 2c 22 54 79 70 65 22  3a 22 53 4d 53 22 2c 22   ","Type" :"SMS","
02a0  54 72 61 63 6b 49 64 22  3a 22 35 34 37 37 38 38   TrackId" :"547788
02b0  30 33 22 2c 22 55 6e 72  65 61 64 43 6f 75 6e 74   03","Unr eadCount
02c0  22 3a 22 31 22 2c 22 4d  73 67 43 6f 6d 70 6c 65   ":"1","M sgComple
02d0  74 65 64 22 3a 22 59 22  2c 22 54 69 6d 65 73 74   ted":"Y" ,"Timest
02e0  61 6d 70 22 3a 22 31 33  38 30 39 34 32 39 34 37   amp":"13 80942947
02f0  22 2c 22 4d 69 73 73 65  64 43 61 6c 6c 73 43 6f   ","Misse dCallsCo
0300  75 6e 74 22 3a 22 30 22  7d                        unt":"0" }
```

Fig. 5 Plain text mobile number and conversation in Vonage text message

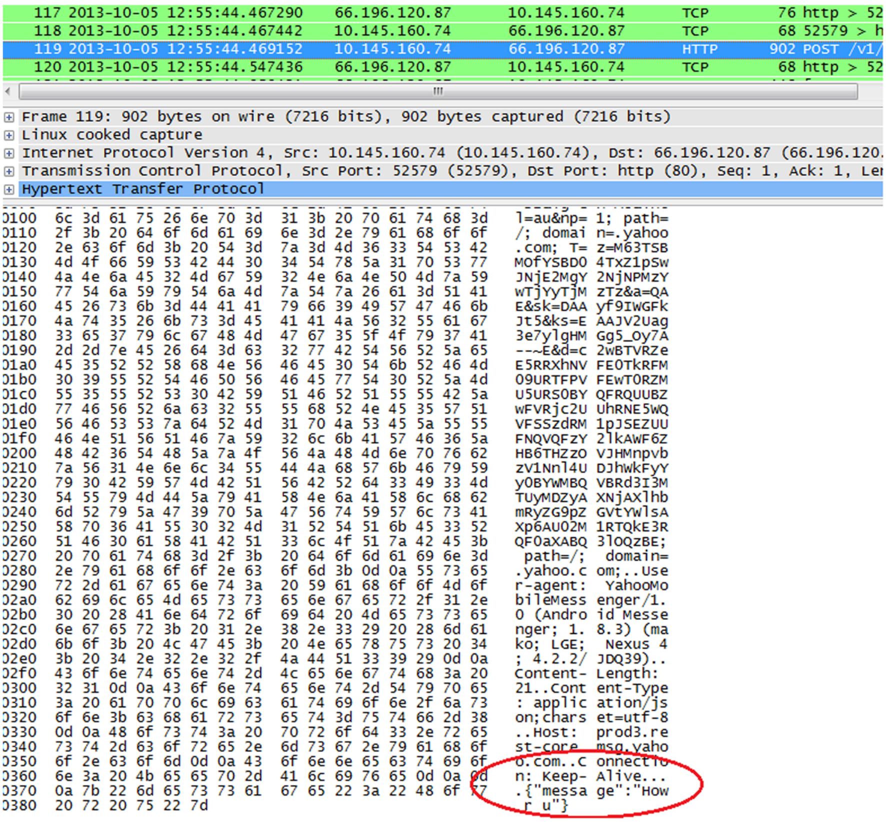
5.2 Voice data analysis using histogram

The results of histogram analysis of the captured voice data for m2 m communications are shown in Appendix Figs. 7 and 8. The histograms for Skype were consistent in both samples. The bytes were evenly distributed in both samples for Skype (i.e. approximately 25,000 occurrences of each byte). There is no cluster in any region of the histograms, which suggests that Skype m2m voice communications are encrypted.

For Google Hangout, the histogram analysis showed frequency distribution of bytes with no clusters for both samples. The bytes were evenly distributed and approximately 15,000 occurrences of each byte were observed in both samples. This suggests that Google Hangout m2m voice communications are encrypted.

For ICQ, a small cluster was shown at the region 0 × FA in both samples. The clusters were marked with circles. The bytes were evenly distributed and approximately 15,000 occurrences of each byte were observed in both samples. However, the byte distribution increased to approximately 17,000 occurrences in the clustered region (0 × FA).This indicates that ICQ voice data are not encrypted while using mobile data network at both ends.

The histogram for Viber showed clusters in the region 0 × C8 for both samples 1 and 2 (see Appendix Figs. 7 and 8). Other regions had even byte distribution. The



```
117 2013-10-05 12:55:44.467290   66.196.120.87   10.145.160.74   TCP    76 http > 52
118 2013-10-05 12:55:44.467442   10.145.160.74   66.196.120.87   TCP    68 52579 > h
119 2013-10-05 12:55:44.469152   10.145.160.74   66.196.120.87   HTTP  902 POST /v1/
120 2013-10-05 12:55:44.547436   66.196.120.87   10.145.160.74   TCP    68 http > 52

⊞ Frame 119: 902 bytes on wire (7216 bits), 902 bytes captured (7216 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 10.145.160.74 (10.145.160.74), Dst: 66.196.120.87 (66.196.120.
⊞ Transmission Control Protocol, Src Port: 52579 (52579), Dst Port: http (80), Seq: 1, Ack: 1, Ler
⊞ Hypertext Transfer Protocol

0100  6c 3d 61 75 26 6e 70 3d  31 3b 20 70 61 74 68 3d   l=au&np= 1; path=
0110  2f 3b 20 64 6f 6d 61 69  6e 3d 2e 79 61 68 6f 6f   /; domai n=.yahoo
0120  2e 63 6f 6d 3b 20 54 3d  7a 3d 4d 36 33 54 53 42   .com; T= z=M63TSB
0130  4d 4f 66 59 53 42 44 30  34 54 78 5a 31 70 53 77   MOfYSBD0 4TxZ1pSw
0140  4a 4e 6a 45 32 4d 67 59  32 4e 6a 4e 50 4d 7a 59   JNjE2MgY 2NjNPMzY
0150  77 54 6a 59 79 54 6a 4d  7a 54 7a 26 61 3d 51 41   wTjYyTjM zTz&a=QA
0160  45 26 73 6b 3d 44 41 41  79 66 39 49 57 47 46 6b   E&sk=DAA yf9IWGFk
0170  4a 74 35 26 6b 73 3d 45  41 41 4a 56 32 55 61 67   Jt5&ks=E AAJV2Uag
0180  33 65 37 79 6c 67 48 4d  47 67 35 5f 4f 79 37 41   3e7ylgHM Gg5_Oy7A
0190  2d 2d 7e 45 26 64 3d 63  32 77 42 54 56 52 5a 65   --~E&d=c 2wBTVRZe
01a0  45 35 52 52 58 68 4e 56  46 45 30 54 6b 52 46 4d   E5RRXhNV FE0TkRFM
01b0  30 39 55 52 54 46 50 56  46 45 77 54 30 52 5a 4d   09URTFPV FEwT0RZM
01c0  55 35 55 52 53 30 42 59  51 46 52 51 55 55 42 5a   U5URS0BY QFRQUUBZ
01d0  77 46 56 52 6a 63 32 55  55 68 52 4e 45 35 57 51   wFVRjc2U UhRNE5WQ
01e0  56 46 53 53 7a 64 52 4d  31 70 4a 53 45 5a 55 55   VFSSzdRM 1pJSEZUU
01f0  46 4e 51 56 51 46 7a 59  32 6c 6b 41 57 46 36 5a   FNQVQFzY 2lkAWF6Z
0200  48 42 36 54 48 5a 7a 4f  56 4a 48 4d 6e 70 76 62   HB6THZzO VJHMnpvb
0210  7a 56 31 4e 6e 6c 34 55  44 4a 68 57 6b 46 79 59   zV1Nnl4U DJhWkFyY
0220  79 30 42 59 57 4d 42 51  56 42 52 64 33 49 33 4d   y0BYWMBQ VBRd3I3M
0230  54 55 79 4d 44 5a 79 41  58 4e 6a 41 58 6c 68 62   TUyMDZyA XNjAXlhb
0240  6d 52 79 5a 47 39 70 5a  47 56 74 59 57 6c 73 41   mRyZG9pZ GVtYWlsA
0250  58 70 36 41 55 30 32 4d  31 52 54 51 6b 45 33 52   Xp6AU02M 1RTQkE3R
0260  51 46 30 61 58 41 42 51  33 6c 4f 51 7a 42 45 3b   QF0aXABQ 3lOQzBE;
0270  20 70 61 74 68 3d 2f 3b  20 64 6f 6d 61 69 6e 3d    path=/;  domain=
0280  2e 79 61 68 6f 6f 2e 63  6f 6d 3b 0d 0a 55 73 65   .yahoo.c om;..Use
0290  72 2d 61 67 65 6e 74 3a  20 59 61 68 6f 6f 4d 6f   r-agent:  YahooMo
02a0  62 69 6c 65 4d 65 73 73  65 6e 67 65 72 2f 31 2e   bileMess enger/1.
02b0  30 20 28 41 6e 64 72 6f  69 64 20 4d 65 73 73 65   0 (Andro id Messe
02c0  6e 67 65 72 3b 20 31 2e  38 2e 33 29 20 28 6d 61   nger; 1. 8.3) (ma
02d0  6b 6f 3b 20 4c 47 45 3b  20 4e 65 78 75 73 20 34   ko; LGE;  Nexus 4
02e0  3b 20 34 2e 32 2e 32 2f  4a 44 51 33 39 29 0d 0a   ; 4.2.2/ JDQ39)..
02f0  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length:
0300  32 31 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   21..Cont ent-Type
0310  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6a 73   : applic ation/js
0320  6f 6e 3b 63 68 61 72 73  65 74 3d 75 74 66 2d 38   on;chars et=utf-8
0330  0d 0a 48 6f 73 74 3a 20  70 72 6f 64 33 2e 72 65   ..Host:  prod3.re
0340  73 74 2d 63 6f 72 65 2e  6d 73 67 2e 79 61 68 6f   st-core. msg.yaho
0350  6f 2e 63 6f 6d 0d 0a 43  6f 6e 6e 65 63 74 69 6f   o.com..C onnectio
0360  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 0d   n: Keep- Alive...
0370  0a 7b 22 6d 65 73 73 61  67 65 22 3a 22 48 6f 77   .{"messa ge":"How
0380  20 72 20 75 22 7d                                   r u"}
```

Fig. 6 Plain text conversation in Yahoo text message

clustered region had approximately 20,000 occurrences for each byte, whereas the other regions had approximately 18,000 occurrences. The clustered regions reflect the scrambling mechanism used by Viber.

The analysis of Nimbuzz data did not reveal any clusters in any region. The bytes were evenly distributed in both samples (i.e. approximately 10,000 occurrences of each byte), which indicates Nimbuzz m2m voice communications are encrypted.

The results from the analysis of the captured Yahoo voice data showed even distribution of the bytes in sample 2 with no cluster in any region but there was a cluster in the region 0 × 64 in sample 1. The clustered region in sample 1 had approximately 10,000 occurrences for each byte, whereas sample 2 had a uniform distribution of bytes with approximately 7500 occurrences for each byte. This suggests that Yahoo m2m voice communications are not encrypted.

On the other hand, analysis of Fring data indicated that there were clusters in the 0 × 80 region in both samples. The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. This suggests that Fring m2m voice communications are not encrypted.

Vonage voice data showed even distribution of the bytes with approximately 10,000 occurrences for each byte in sample 1 with no cluster in any region, but there was a cluster in the region 0 × E1 in sample 2 (see Appendix Fig. 8).The approximate number of occurrences for each byte was 10,000 in sample 2, but the clustered region had approximately 12,500 occurrences for each byte. The presence of these clusters suggested that Vonage m2m voice communications are not encrypted.

The analysis of WeChat data showed a cluster in sample 1 in region 0 × FA and in sample 2 in region 0 × 23. The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. The presence of these clusters suggested that WeChat m2m voice communications are not encrypted.

Tango voice data histogram analysis showed two clusters in both samples. For samples 1 and 2, the clusters appeared in regions 0 × 64 and 0 × 90, and regions 0 × 36 and 0 × 64 respectively (see Appendix Figs. 7 and 8). The clustered region had approximately 30,000 occurrences for each byte, whereas the other regions had approximately 20,000 occurrences. The presence of these pair of clusters in both samples suggested that Tango does not encrypt m2m voice communications.

5.3 Voice data analysis using entropy

The entropy analysis of the first sample of Skype data produced a result of 5.5–6.5 bits per character for m2m voice communication with very few sudden drifts (see Appendix Fig. 9). In the second sample, the variation in entropy was again between 5.5 and 6.5 bits per character with no sudden drifts (see Appendix Fig. 10). The change in entropy was even and the value varied within 1.0 bit per character for both samples. An even distribution of entropy suggests that Skype m2m voice communications are encrypted.

For Google Hangout, the entropy results were between 5.0 and 6.8 bits per character for sample 1, and 5.3–6.6 bits per character for sample 2. The fluctuation was higher than Skype. As shown in Appendix Figs. 9 and 10, the fluctuation occurred slowly. There was no sudden spike in the entropy. However, there was a sudden drift in the second sample, which is most probably an outlier due to background noise introduced during the capturing of the second audio sample. Therefore, Google Hangout m2m voice communications are encrypted.

Results from ICQ were interesting. As shown in Appendix Fig. 9, there was a continuous fluctuation within the range of 6.0–7.2 bits per character for the first sample. In the second sample, there was a continuous change of entropy from 5.0–7.0 bits per character during the beginning, and then it remained steady within the range 6.6–7.3 bits per character (see Appendix Fig. 10). The uneven distribution of entropy suggests that ICQ m2m voice communications are not encrypted.

Viber also produced an uneven entropy distribution within the range of 2.5–7.0 bits per character for both samples. The fluctuation was very high and the entropy change was continuous. The uneven distribution of entropy suggests that Viber m2m voice communications are not encrypted.

The entropy analysis results of Nimbuzz had a steady distribution within the range of 5.5–6.0 bits per character in both samples. However, there were sudden drifts in the entropy for both samples, which were likely outliers. Overall, the entropy distribution was very even. The even distribution of entropy suggests that Nimbuzz m2m voice communications are encrypted.

Yahoo had a relatively low entropy distribution with the entropy varying from 4.2 to 5.9 bits per character in both samples. But, in sample 2, the entropy remained constant within 5.4–5.9 bits per character during the first half of the analysis (see Appendix Fig. 10). Other than that, the entropy hardly remained steady and fluctuations were observed throughout the communication sessions. The uneven distribution of entropy suggests that Yahoo m2m voice communications are not encrypted.

The entropy analysis of Fring produced highly varying entropy values between 2.0 and 6.5 bits per characters throughout the analysis for both samples. Lack of steadiness was observed in both samples, which indicates that Fring m2m voice communications are not encrypted.

The overall entropy distributions for Vonage were around the range of 4.5–7.0 bits per character for both samples. Sudden drifts were observed in the entropy analysis. For WeChat, the entropy results varied in the range of 5.0–6.8 bits per character. Both Vonage and WeChat had uneven distribution of entropy, suggesting that the m2m voice communications are not encrypted.

The entropy analysis of Tango produced entropy in range of 3.9–6.5 bits per character for sample 1 and 4.8–6.7 bits per character for sample 2 with a couple of sudden drifts for both samples (see Appendix Figs. 9 and 10). The highly varying entropy distribution indicates that Tango m2m voice communications are not encrypted.

6 Findings from mobile data network to WiFi network (m2w) communications

6.1 Text data analysis

For Fring and Vonage, the mobile number of the sender was visible. This was surprising because we were using WiFi network at the receiving end. We believe that this is due to the fact that both Fring and Vonage use the number of the mobile handset for authentication and as user ID (see Table 1). We observed that the mobile phone number of the sender and the text messages were also in plaintext in our experiments (see Figs. 4, 5). For Yahoo, only the messages were in plaintext (see Fig. 6). For Tango, the mobile phone number was in plaintext, but there was no information about the messages as discussed in Sect. 5.1. The remaining six mVoIP apps, namely Skype, Google Hangout, ICQ, Viber, Nimbuzz and WeChat, provided no clue about the sender or receiver or the contents of the communication.

6.2 Voice data analysis using histogram

The analysis of the captured voice data with pcap histogram for m2w communication is shown in Appendix Figs. 11 and 12. The histograms for Skype and Google Hangout were consistent in both samples. The results for Skype and Google Hangout histogram analysis were identical as the results discussed in Sect. 5.2.

The bytes were evenly distributed in both samples for Skype and Google hangout (i.e. approximately 25,000 occurrences of each byte for Skype and 15,000 for Google hangout). There is no cluster in any region of the histograms, which suggests that Skype and Google VoIP are encrypted for m2w voice communications.

For ICQ and Viber, the results were identical as the results discussed in Sects. 5.2. A small cluster was shown in the region 0 × FA in both samples of ICQ (see Appendix Figs. 11 and 12). The bytes were evenly distributed, with approximately 15,000 occurrences of each byte in both samples of ICQ. However, we observed that the byte distribution increased to approximately 17,000 occurrences in the clustered region (0 × FA).The histogram of the sessions captured for Viber showed clusters in the region 0 × C8 for both sample 1 and sample 2. The clustered region had approximately 20,000 occurrences for each byte, whereas the other regions had approximately 18,000 occurrences. This indicates that ICQ and Viber voice m2w communications are not encrypted.

However, the analysis of Nimbuzz voice data was not similar to the findings reported in Sect. 5.2. There was no cluster in any region in sample 1 but there was a cluster around the region 0 × 64 in sample 2 (see Appendix Fig. 12). The bytes were evenly distributed, with approximately 10,000 occurrences of each byte in both samples of Nimbuzz. However, we observed that the byte distribution increased to approximately 15,000 occurrences in the clustered region in sample 2. This indicates that Nimbuzz voice m2w communications are not encrypted.

The results from the analysis of the captured Yahoo voice data showed even distribution of the bytes in both samples with no cluster in any region. The bytes were evenly distributed in both samples (i.e. approximately 7500 occurrences of each byte), which indicates yahoo m2w voice communications are encrypted.

On the other hand, analysis of Fring data indicated that there were clusters in the region 0 × 20 in both samples. The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. This suggests that Fring m2w voice communications are not encrypted.

Vonage voice data showed clusters in the region 0 × F5 in both samples (see Appendix Figs. 11 and 12). The approximate number of occurrences for each byte was 10,000 in both samples, but the clustered region had approximately 12,500 occurrences for each byte. The presence of the clusters in the samples indicates Vonage m2w voice communications are not encrypted.

The analysis of WeChat data showed a cluster in sample 1 in region 0 × FA and in sample 2 in region 0 × 05. The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. The presence of these clusters in WeChat voice data indicates the absence of encryption in m2w voice communications. In addition, a difference in histogram clusters between the two samples is another indication of no encryption.

Tango voice data histogram analysis showed two clusters in both samples as it was found in Sect. 5.2. For sample 1, the clusters appeared in the regions 0 × 38 and 0 × 90 (see Appendix Fig. 11). For sample 2, the clusters appeared in the regions 0 × 36 and 0 × 64 (see Appendix Fig. 12). The clustered region had approximately 30,000 occurrences for each byte, whereas the other regions had approximately 20,000 occurrences. The presence of these pairs of clusters in the samples indicates Tango m2w voice communications are not encrypted.

6.3 Voice data analysis using entropy

The first sample of Skype data produced the entropy of 5.6–6.4 bits per character for m2w voice communication (see Appendix Fig. 13). The second sample resulted in the entropy of 5.7–6.6 bits per character(see Appendix Fig. 14). Although the second sample had some drifts towards the end of the experiment, the overall change in entropy was even and the value varied within 1.0 bit per character for both samples, which indicates Skype m2w voice communications are encrypted.

For Google Hangout, the entropy results were between 4.7 and 6.8 bits per character for samples 1. There was no sudden spike in the entropy. The entropy distribution was even, which indicates Google Hangout m2w voice communications are encrypted.

The first sample of ICQ data had an entropy range of 5.4–5.8 bits per character with a sudden drift. In the second sample, there was a continuous change of entropy from 5.4 to 6.5 bits per character during the beginning, and then it climbed to 7.0 bits per character before dropping again to 6.0 bits per character. There was also a sudden drift towards the end. The uneven distribution of entropy suggests that ICQ m2w voice communications are not encrypted.

Viber also produced an uneven entropy distribution within the range of 2.5–7.0 bits per character for both samples (see Appendix Figs. 13 and 14). The results were similar as found in Sect. 5.2. The uneven distribution of entropy suggests that Viber m2w voice communications are not encrypted.

The entropy analysis results of Nimbuzz had a distribution within the range 5.5–7.0 bits per character in sample 1. But there were sudden spikes in the entropy in the entropy. For sample 2, the entropy distribution was steady between 5.6 and 5.9 bits per character with one sudden drift (see Appendix Figs. 13 and 14). We assume that the sudden drift of entropy is an outlier, as the entropy is evenly distributed throughout. This suggests that Nimbuzz m2w voice communications are encrypted.

Yahoo had a relatively low entropy distribution with the entropy varying from 4.2 to 5.9 bits per character in both samples. The entropy hardly remained steady and fluctuations were observed throughout the communication session. The uneven distribution of entropy suggests that Yahoo m2w voice communications are not encrypted.

The entropy analysis of Fring produced highly varying entropy between 2.0 and 6.5 bits per characters throughout the analysis for both samples (see Appendix Figs. 13 and 14). Lack of steadiness was observed in both samples. Lack of steadiness was observed in both samples, which indicates that Fring m2w voice communications are not encrypted.

The overall entropy distributions for Vonage were around the range of 5.5–7.0 bits per character for sample 1. The entropy distribution was between 6.2 and 7.0 bits per character in sample 2 with sudden drifts in distribution. Due to the uneven distribution of entropy, Vonage m2w voice communications does not appear to be encrypted.

For WeChat, the entropy results varied in the range of 5.0–7.0 bits per character for both samples. There was a continuous change of entropy, which indicates that WeChat m2w voice communications are not encrypted.

Tango's entropy is in the range of 5.0–6.5 bits per character for sample 1 and 4.0–6.5 bits per character for sample 2 with a couple of sudden drifts for both samples (see Appendix Figs. 13 and 14). We assumed that the sudden drift of entropy is an outlier. Based on the observation that the entropy is evenly distributed, Tango m2w voice communications appeared to be encrypted.

7 Findings from WiFi network to mobile data network (w2m) communication

7.1 Text data analysis

The text message analysis of WiFi network at the sender's end (the device where the pcap packets are captured) and mobile data network at the receiver's end provided the following results. For Fring and Vonage, the received messages were in plaintext and the mobile phone number was also visible as discussed in Sects. 5.1 and 6.1. For Yahoo, only the messages were in plaintext, as it was reported in Sects. 5.1 and 6.1. However, unlike the results in Sects. 5.1 and 6.1, the mobile phone number of the phone using mobile data network and the phone using WiFi network was not visible in plaintext for Tango. The remaining six mVoIP apps, namely Skype, Google Hangout, ICQ, Viber, Nimbuzz and WeChat, revealed no plaintext data or any clue about the sender or receiver. Similar findings were reported in Sects. 5.1 and 6.1.

7.2 Voice data analysis using histogram

The results for Skype and Google Hangout histogram analysis are similar to the findings reported in Sects. 5.2 and 6.2. The histograms for Skype and Google Hangout were consistent in both samples. The bytes were evenly distributed in both samples for Skype and Google hangout (i.e. approximately 25,000 occurrences of each byte for Skype and 10,000 for Google hangout). There is no cluster in any region of the histograms (see Appendix Figs. 15 and 16), which suggests that Skype and Google Hangout VoIP are encrypted in the w2m voice communications.

For ICQ and Viber, the results were similar to the findings reported in Sects. 5.2 and 6.2. A small cluster was shown in the region 0 × FA in both samples of ICQ (see Appendix Figs. 15 and 16). The bytes were evenly distributed, with approximately 15,000 occurrences of each byte observed in both samples of ICQ. However, the byte distribution increased to approximately 17,000 occurrences in the clustered region (0 × FA).The histogram of the sessions captured for Viber showed clusters in the region 0 × C8 for both samples (see Appendix Figs. 15 and 16). The clustered region had approximately 20,000 occurrences for each byte, whereas the other regions had approximately 18,000 occurrences for the bytes. This suggested that ICQ and Viber w2m voice communications are not encrypted.

However, the analysis of Nimbuzz and Yahoo voice data revealed no cluster in any region in both samples (see Appendix Figs. 15 and 16). The bytes were evenly distributed in both samples (i.e. approximately 10,000 occurrences of each byte) for both Nimbuzz and Yahoo, which indicates Nimbuzz and Yahoo w2m voice communications are encrypted.

The analysis of Fring data indicated that there were clusters in the region 0 × 20 in sample 1 (see Appendix Figs. 15) and in region 0 × 80 in sample 2 (see Appendix Figs. 16). The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. This suggests that Fring w2m voice communications are not encrypted.

Vonage voice data showed no cluster in both samples. The bytes were evenly distributed in both samples (i.e. approximately 10,000 occurrences of each byte).The analysis of WeChat data showed a cluster in sample 1 in region 0 × 05 and in sample 2 in region 0 × FA. The clustered region had approximately 15,000 occurrences for each byte, whereas the other regions had approximately 10,000 occurrences. The presence of these clusters in WeChat voice data suggested that w2m voice communications are not encrypted.

Tango voice data histogram analysis showed two clusters in both samples—similar to the findings reported in Sects. 5.2 and 6.2. For sample 1, the clusters appeared in the regions 0 × 38 and 0 × 90 (see Appendix Fig. 15). For sample 2, the clusters appeared in the regions 0 × 36 and 0 × 64 (see Appendix Fig. 16).The clustered region had approximately 30,000 occurrences for each byte, whereas the other regions had approximately 20,000 occurrences. The presence of these pairs of clusters and a difference in histogram clusters between the two samples indicate lack of encryption in Tango voice in w2m communication.

7.3 Voice data analysis using entropy

The entropy analysis of the first sample of Skype data produced a result of 5.5–6.5 bits per character for w2m communication (see Appendix Fig. 17). In the second sample, the variation in entropy was between 6.0 and 6.8 bits per character (see Appendix Fig. 18). The change in entropy was even and the value varied within 1.0 bit per character for both samples, indicating that the Skype w2m communications are encrypted.

For Google Hangout, the entropy results were between 5.0 and 7.0 bits per character. The fluctuation was higher than Skype. As shown in Appendix Figs. 17 and 18, the fluctuation occurred slowly. There was no sudden spike in the entropy. The entropy was consistent around the region between 5.0 and 7.0 bits per character. However, there is a sudden drift, which can be classified as outlier due to network noise. Therefore, Google Hangout w2m voice communications appeared to be encrypted.

Results from ICQ were inconsistent. There was a continuous fluctuation within the range of 5.5–7.2 bits per character. In other words, there is an uneven distribution of entropy throughout the communication sessions. As shown in Appendix Figs. 17 and 18, the entropy distribution is constantly changing. The uneven distribution of entropy suggested that ICQ w2m voice communications are not encrypted.

Viber also produced an uneven entropy distribution within the range of 2.5–7.0 bits per character (see Appendix Figs. 17 and 18). The fluctuation was very high and the entropy change was continuous (as reported in Sects. 5.2 and 6.2). The uneven distribution of entropy suggests that Viber w2m voice communications are not encrypted.

The entropy analysis results of Nimbuzz had a steady distribution within the range 5.5–5.9 bits per character in sample 1 and 5.6–5.8 bits per character in sample 2. But there were sudden drifts in the entropy for both samples towards the third quarter of the communication session. These two drifts can be considered as outliers. Overall, the entropy distribution was very even, which suggests that Nimbuzz w2m voice communications are encrypted.

Yahoo had a relatively low entropy distribution with the entropy varying from 4.0 to 5.8 bits per character in sample 1 and 4.2 to 5.7 bits per character in sample 2. The entropy hardly remained steady and fluctuations were observed throughout the communication session. The uneven distribution of entropy suggests that Yahoo w2m voice communications are not encrypted.

The entropy analysis of Fring produced highly varying entropy between 2.5 and 6.5 bits per characters throughout the analysis for both samples (see Appendix Figs. 17 and 18). Lack of steadiness was observed in both samples. The uneven distribution of entropy suggests that Fring w2m voice communications are not encrypted.

The overall entropy distributions for Vonage were around the range of 4.5 and 7.0 bits per character in for both samples. Sudden drifts were observed in the entropy analysis. For WeChat, the entropy results varied in the range of 5.5 and 7.0 bits per character (see Appendix Figs. 17 and 18). Both Vonage and WeChat had uneven distribution of entropy, indicating that the w2m voice communications are not encrypted.

The entropy analysis of Tango produced entropy in range of 5.0–7.0 bits per character for both samples with a couple of sudden drifts for both samples (see Appendix Figs. 17 and 18). Other than these couple of drifts, the entropy was steady. An even distribution of entropy suggests that Tango w2m voice communications are encrypted.

8 Discussion

Employees from various industries including but not limited to consultancy, health, mining and government use mVoIP apps (e.g. Skype) to communicate with their stakeholders and customers [40]. For example, mVoIP communication may be used to connect a customer to a live agent to provide electronic Customer Relationship Management (eCRM) services [11]. Due to the lack of vendor documentations, users are generally unaware of whether their communication is encrypted or not. We found only four apps—Skype, Google Hangout, ICQ and Viber provide relevant vendor documentations. According to these documentations, Skype and Google Hangout provide encrypted text and voice communications, and Viber provides only encrypted text communications. These assertions are confirmed in our study—see Table 3. Although ICQ documentation suggests that the service does not provide encryption [24], our findings indicate that text communications are encrypted—see Table 3. Security and privacy concerns, as identified in various studies (e.g. [20, 41]), are dominating factors that prevent a broader adoption of mVoIP services in e-commerce. For example, an organisation providing telecare and telehealth services through Skype or any other mVoIP app needs to ensure that their conversations are secure and the services comply with the relevant health information privacy regulations, such as the *Health Insurance Portability and Accountability Act* for US organisations, and the *Privacy Act 1988* (Cth) for Australian organisations.

Table 3 Summary of the findings

Android mVoIP apps	Encryption of (text/voice)	Communication channel			
		w2w [4]	m2m	m2w	w2m
Skype	Text	Y	Y	Y	Y
	Voice	Y	Y	Y	Y
Google Hangout	Text	Y (Google Talk)	Y	Y	Y
	Voice	Y (Google Talk)	Y	Y	Y
ICQ	Text	Y	Y	Y	Y
	Voice	N	N	N	N
Viber	Text	Y	Y	Y	Y
	Voice	N	N	N	N
Nimbuzz	Text	Y	Y	Y	Y
	Voice	Y	Y	Y	Y
Yahoo	Text	N	N	N	N
	Voice	N	N	N	N
Fring	Text	***Y***	***N***	***N***	***N***
	Voice	N	N	N	N
Vonage	Text	***Y***	***N***	***N***	***N***
	Voice	N	N	N	N
WeChat	Text	Y	Y	Y	Y
	Voice	N	N	N	N
Tango	Text	Y	Y	Y	Y
	Voice	***Y***	***N***	***N***	***N***

Bold and Italic representations indicate varying results obtained from the experiments performed for three communication channels (m2m, m2w and w2m) and the experiments performed for w2w communication channel [4]

Secure communication is an area of ongoing research focus. Recently Chang [9] developed a damage compensation index for sustainable security services designed for VoIP services, considered user security and terminal security as major concerns, and assigned both issues a high indexing value. In short, a secure communication implies that an eavesdropper should not be able to recover the contents of the conversation simply by intercepting or capturing the conversation in real-time.

Table 3 summarises the experimental results for all four different communication channels. For w2w communication, Google Talk was considered because Google Hangout replaced Google Talk after the experiments were conducted [4].

As outlined in Table 3, Skype text communications were found to be encrypted and Skype voice communications had no cluster in the histogram analysis with high entropy for each of the three communication channel combinations.

Google Hangout text communications appeared to be encrypted. The voice communications did not have any cluster in the histogram analysis and the entropy results had gradual changes with no sudden rise or fall in entropy in any of the three communication channel combinations. This suggests that Google Hangout encrypts voice communications.

For ICQ, the text communications appeared to be encrypted. Clusters were found in the histogram analysis and the entropy was uneven for each of the four communication channel combination. These findings suggest that ICQ does not encrypt the voice communications.

Viber text communications were determined to be encrypted. The voice communications had cluster in histogram analysis and high fluctuation in entropy analysis for both for each of the four communication channel combinations, which suggest that voice communications are not encrypted.

For Nimbuzz, the text communications were determined to be encrypted. Clusters were found in sample 2 in the m2w communication. No cluster was found in the other communication channel combinations in the histogram analysis. The entropy analysis showed steady changes with very few drifts that can be considered as outliers. The steadiness of entropy results and the absence of cluster in most of the histogram samples strongly suggest that Nimbuzz voice communications are encrypted.

We found Yahoo text communications sent by the user to be in plaintext. No clusters were found in the histograms apart from sample 1 in m2m communication, although the entropy results had high fluctuations. The high fluctuations in entropy suggest that voice communications are not encrypted.

Unlike w2w communications [4], Fring text communications appeared not to be encrypted in m2m, m2w and w2m communications. However, there were clusters found in the histogram analysis with high fluctuation of entropy in the entropy analysis. The results suggest that voice communications are not encrypted in all four communication channel combinations.

Vonage text communications were determined not to be encrypted, whereas the w2w text communications were determined to be encrypted [4]. For m2m voice communications, a cluster was observed only in sample 2. The entropy also varied with sudden drifts. For m2w voice communications, a cluster was observed in each sample and the entropy varied with sudden drifts. For w2m voice communications, there was no cluster in the histograms, but there was a constant variation in entropy change with sudden drifts. Therefore, we believe the voice communications are encoded and not encrypted in all four communication channel combinations.

WeChat text communications appeared to be encrypted. There were clusters in the histograms, and uneven entropy distributions were observed in the entropy analysis. The results suggest that voice communications are not encrypted in all four communication channel combinations.

Finally, Tango text communications appeared to be encrypted. However, several clusters were found in each of the samples for all three communication channel combinations. High variation of entropy was observed in sample 1 of w2w and m2m communications. But the entropy variations were quite steady in other samples. The entropy results suggested that voice communications are encrypted, but the histogram analysis suggested otherwise. Therefore, we believe that voice communications are encoded and not encrypted. However, voice communication was determined to be encrypted for w2w communication [4].

One particularly interesting finding is that three apps (Fring, Vonage, Tango) differ in comparison to w2w communication [4]. Fring and Vonage apps do not appear to encrypt text communications for m2m, m2w and w2m communications, whereas Tango provides encrypted the voice messages only for w2w communication. This indicates that these three mVoIP apps might be silently turning off encryption whenever a mobile network is involved.

In summary, three mVoIP apps (Skype, Google Hangout, and Nimbuzz) appear to encrypt voice data and seven mVoIP apps (Skype, Google Hangout, ICQ, Viber, Nimbuzz, WeChat and Tango) appear to encrypt text communications.

9 Conclusion and future work

The trend of workers increasing mobility is likely to continue, and consequently, mobile and wireless devices will become increasingly important tools for accessing information when desktop computers are unavailable [14]. As technologies become ubiquitous, and smart mobile devices aimed at improving the performance and flexibility of communications proliferate—an era of anywhere–anytime [32]—criminals and other malicious actors will start targeting or continue to target such devices. It is, therefore, important that efforts be made to ensure that all our communication systems have appropriate security measures in place and that users use them to full advantage.

In this paper, we studied one widely used communication system for mobile devices, namely mVoIP apps. We examined ten most popular free mVoIP apps for Android devices in three different communication channel combinations, namely mobile data network to mobile data network (m2m), mobile data network to WiFi network (m2w), and WiFi network to mobile data network (w2m). We determined that Yahoo, Fring and Vonage apps do not encrypt text communications (see Table 3). Using both histogram and entropy analysis, we determined that Skype, Google Hangout, and Nimbuzz encrypt voice data; and ICQ, Viber, Yahoo, Fring, Vonage, WeChat and Tango use some sort of voice encoding mechanism, but does not encrypt the voice data. Our results contribute towards a better understanding of communications using Android mobile VoIP apps.

Our review of academic publications between January 2009 and January 2014 also found that the security and privacy of mVoIP services are an understudied area. There is an ongoing need to conduct more strategic research and evaluation that can provide policy and practice relevant evidence that would enable policy makers, businesses and mVoIP service providers to design national regulatory measures and appropriate policy responses. Future research projects that would help filling gaps in the knowledge base about mVoIP related risks include:

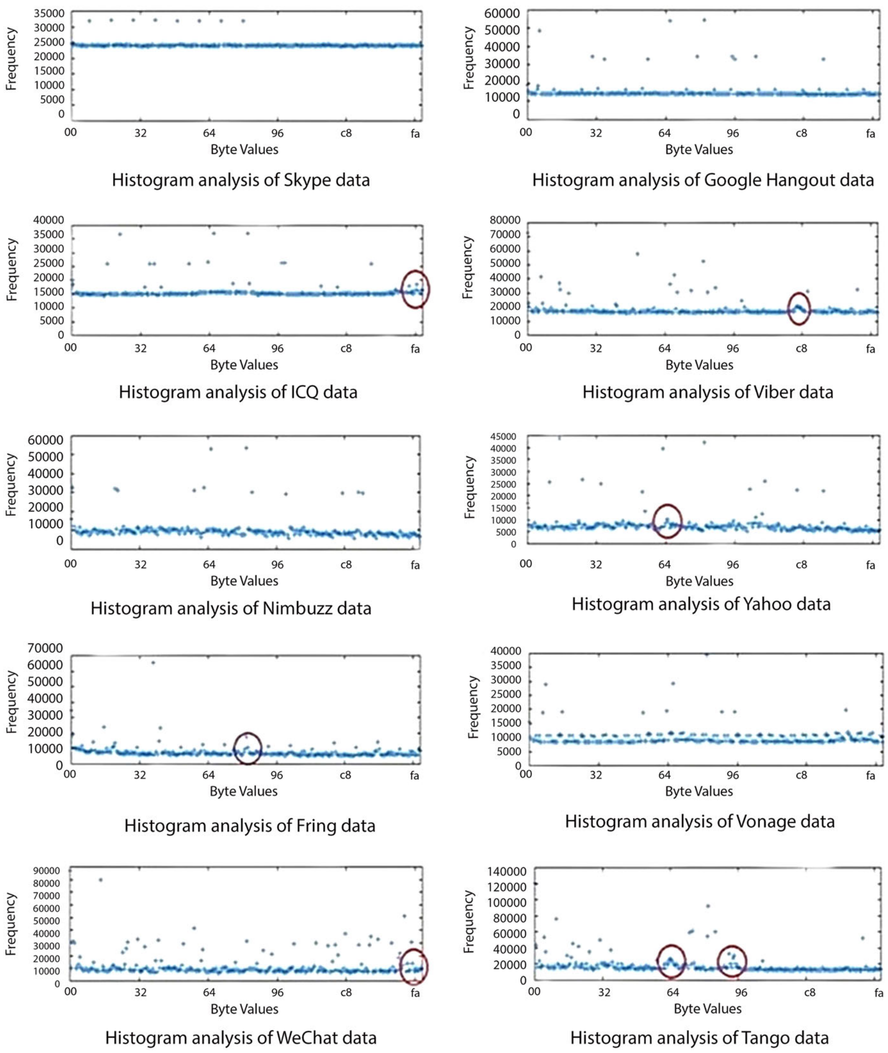
(1) What is the nature of mVoIP related and emerging risks, and how have mobile related risks changed in the past few years?
(2) What are the current trends and emerging challenges that have an impact on mVoIP users?
(3) How can we enhance the security and/or privacy of mVoIP users?
(4) How can we put in place defences to protect even the unaware and/or non-educated mVoIP users?

Another area of interest would be the potential surveillance risks faced by mVoIP and other mobile device users, which is an issue that has attracted international attention in the aftermath of the revelations by Edward Snowden that the National Security Agency has been conducting wide scale government surveillance including those targeting Internet, mobile device and cloud users. Therefore, as suggested by Kim-Kwang Raymond Choo [13], two other key questions that need to be examined are:

(5) How do we balance the need for a secure mobile device and app ecosystem and the rights of individuals to privacy against the need to protect society from serious and organised crimes, terrorism and cyber and national security interests?
(6) What are the implications of user data and personally identifiable information leakage from mobile devices, and should a mobile app provider be responsible for pure economic loss to their users due to its negligence?

Appendix

See Figs. 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18.



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

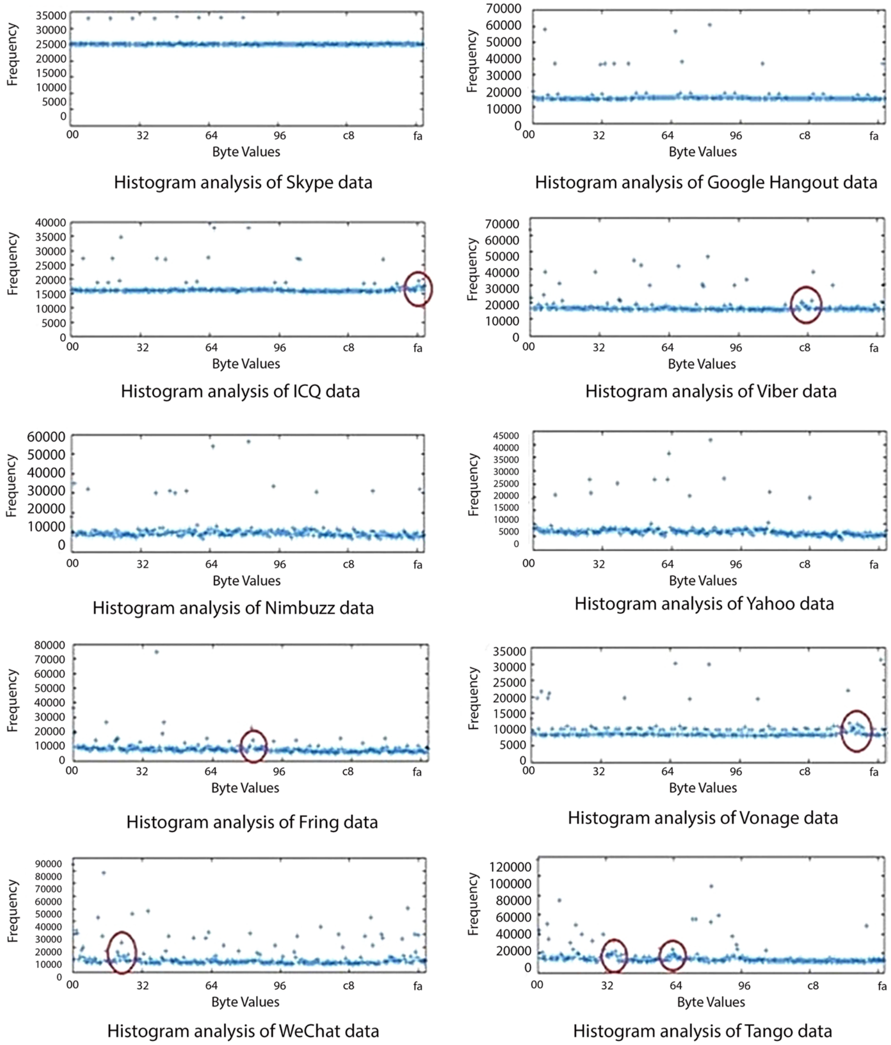
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 7 Histogram analysis of m2m communications (sample 1)



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

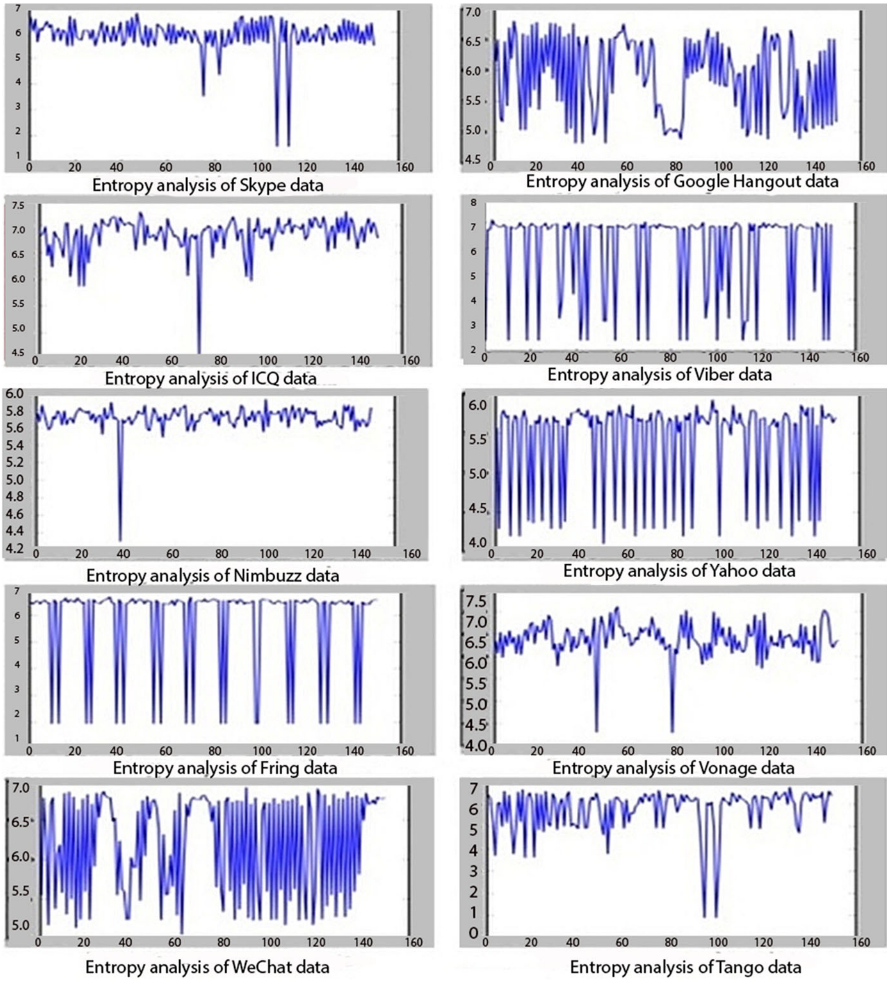
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 8 Histogram analysis of m2m communications (sample 2)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

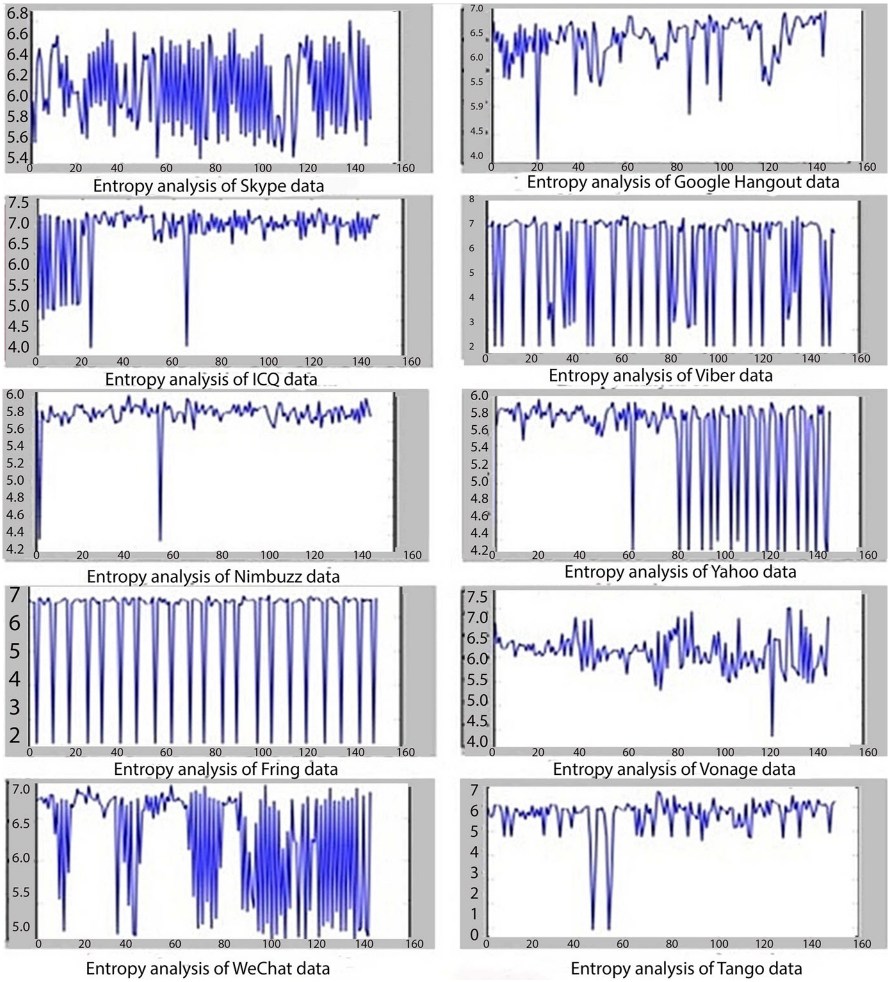
Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 9 Entropy analysis of m2m communications (sample 1)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

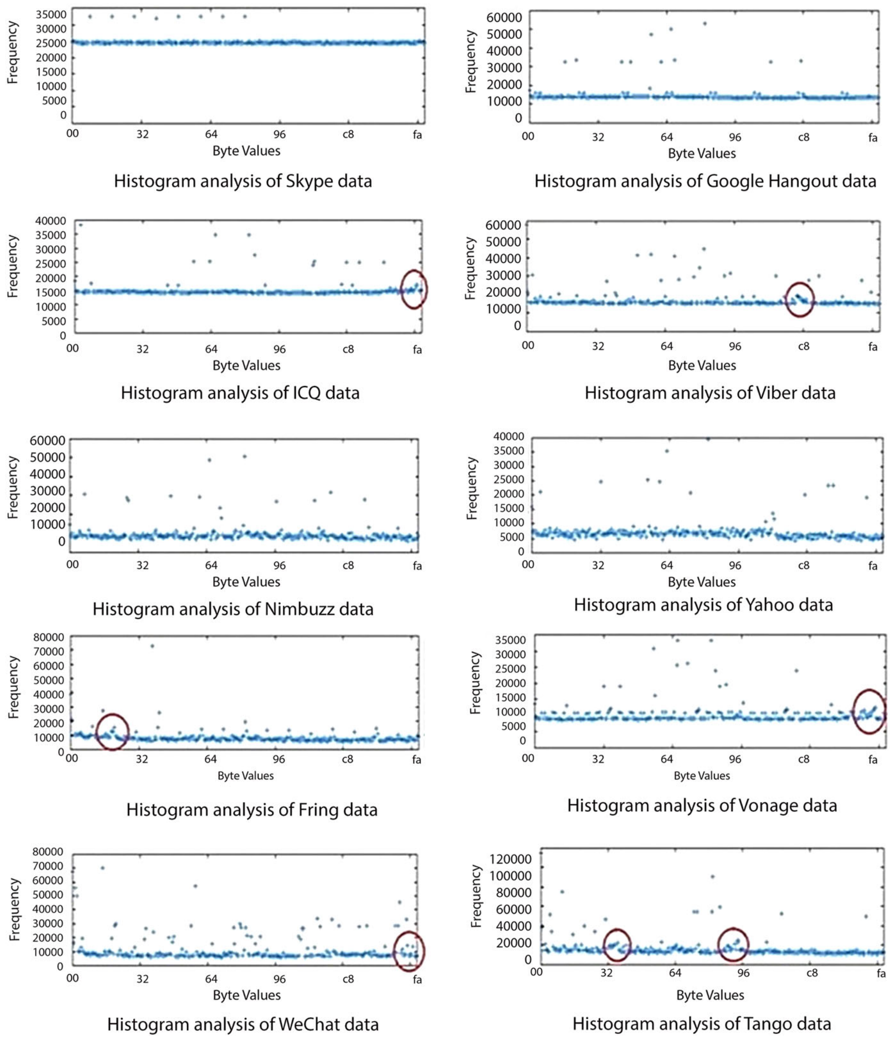
Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 10 Entropy analysis of m2m communications (sample 2)



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

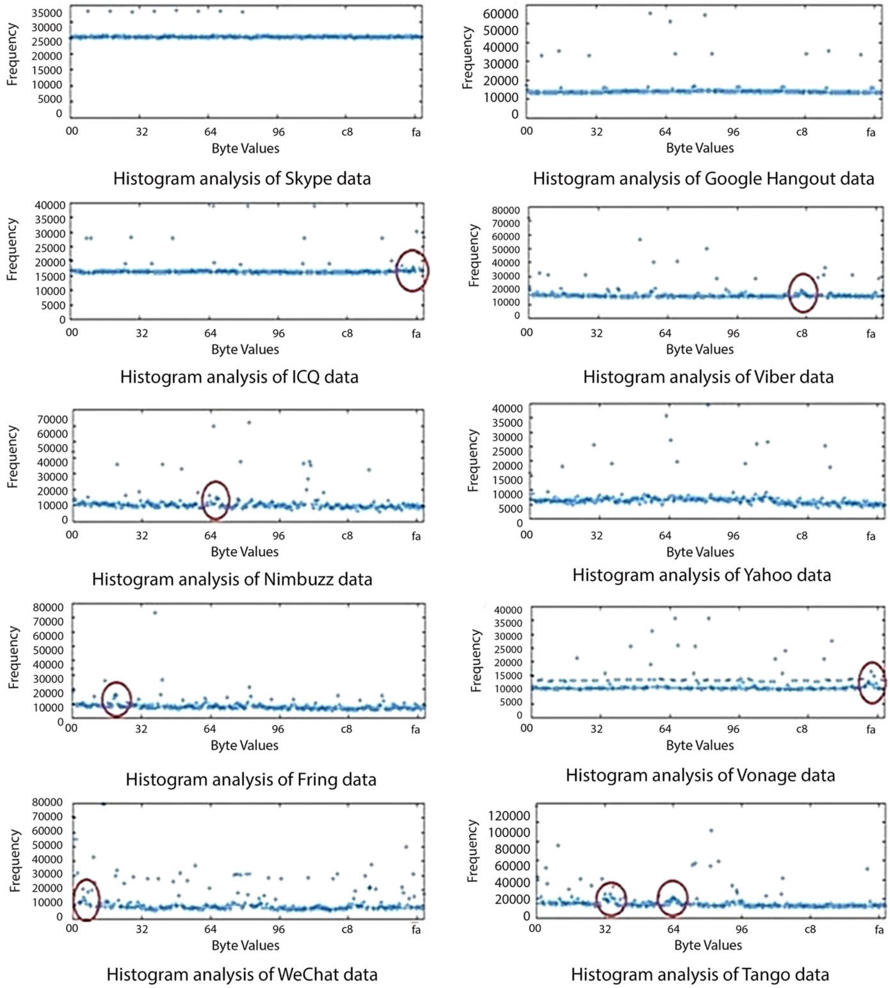
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 11 Histogram analysis of m2w communications (sample 1)



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

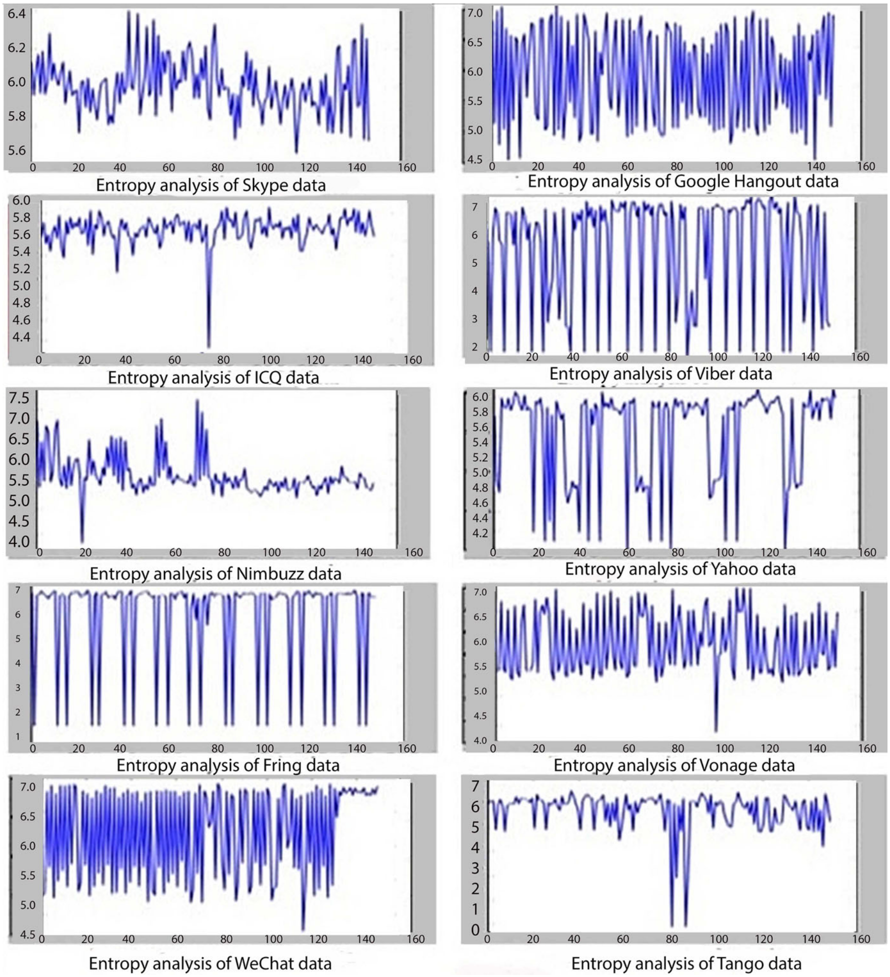
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 12 Histogram analysis of m2w communications (sample 2)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

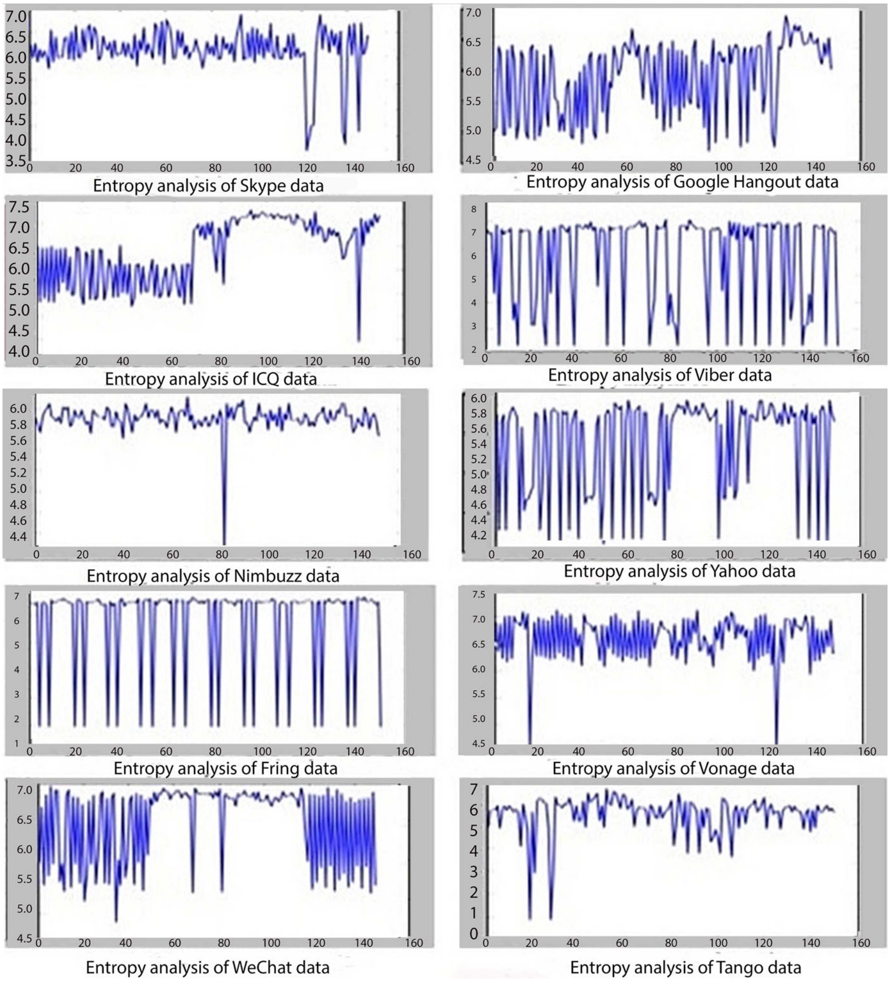
Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 13 Entropy analysis of m2w communications (sample 1)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

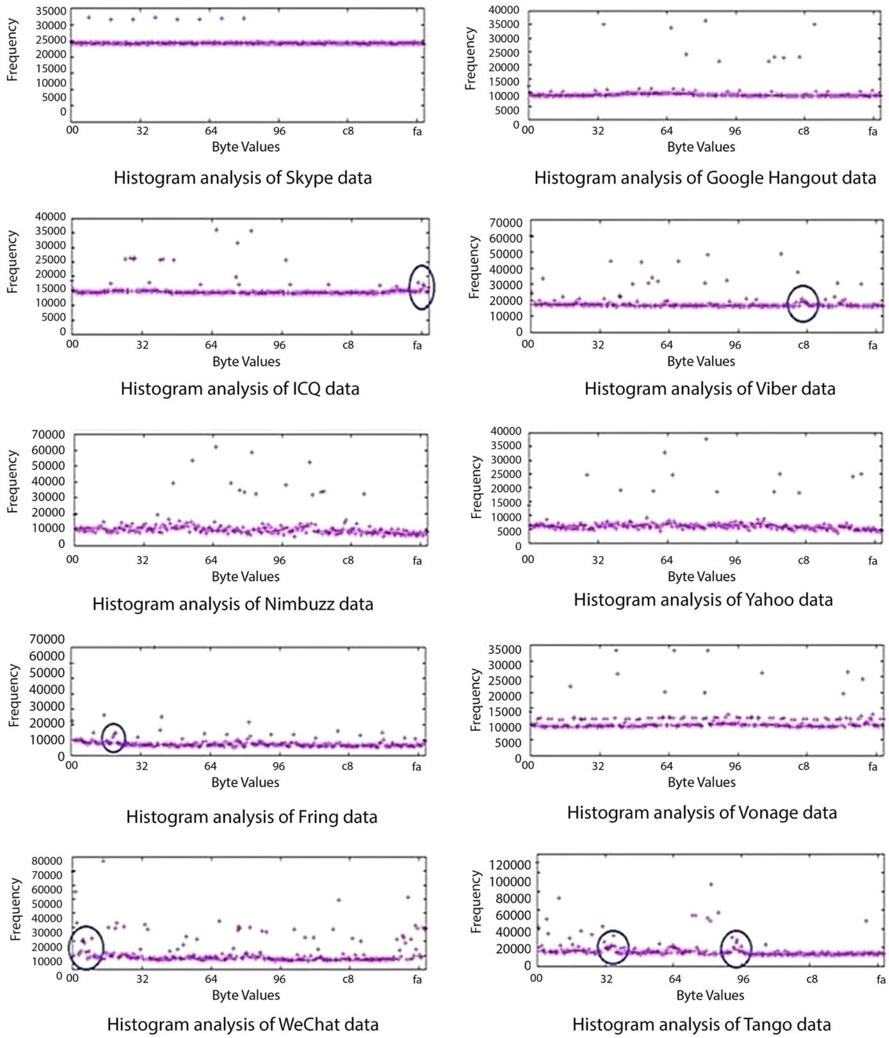
Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 14 Entropy analysis of m2w communications (sample 2)



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

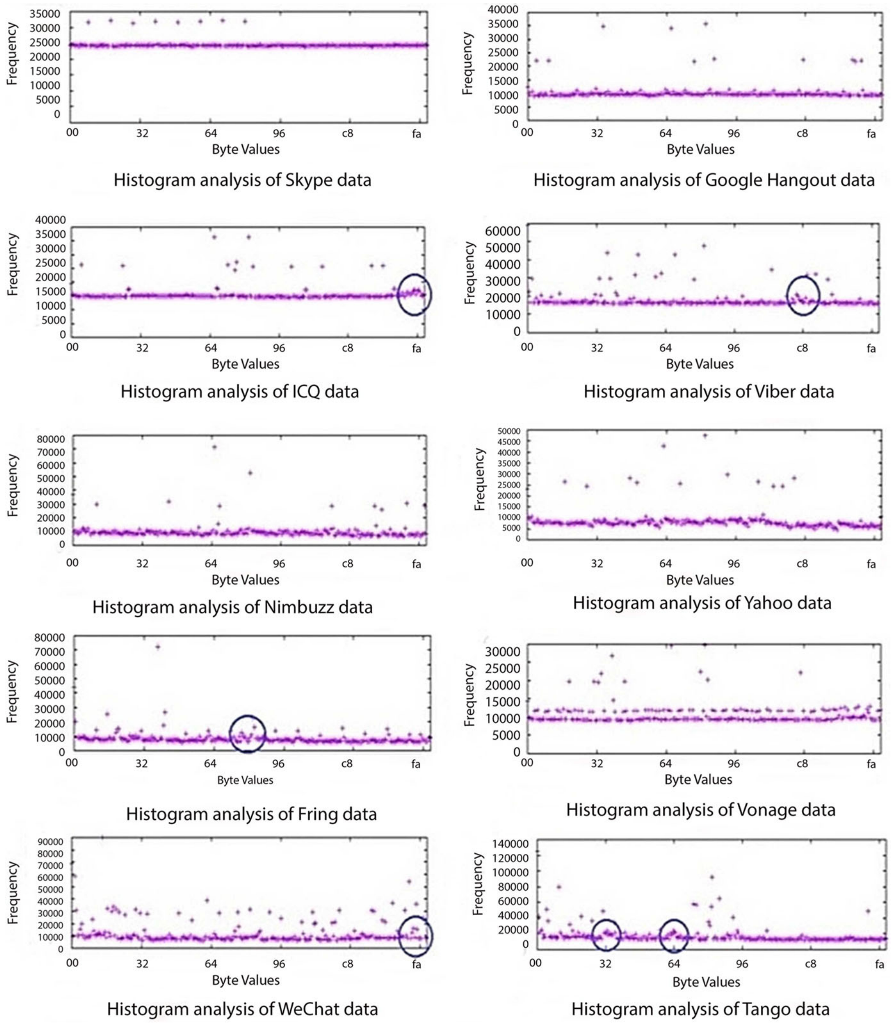
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 15 Histogram analysis of w2m communications (sample 1)



Histogram analysis of Skype data

Histogram analysis of Google Hangout data

Histogram analysis of ICQ data

Histogram analysis of Viber data

Histogram analysis of Nimbuzz data

Histogram analysis of Yahoo data

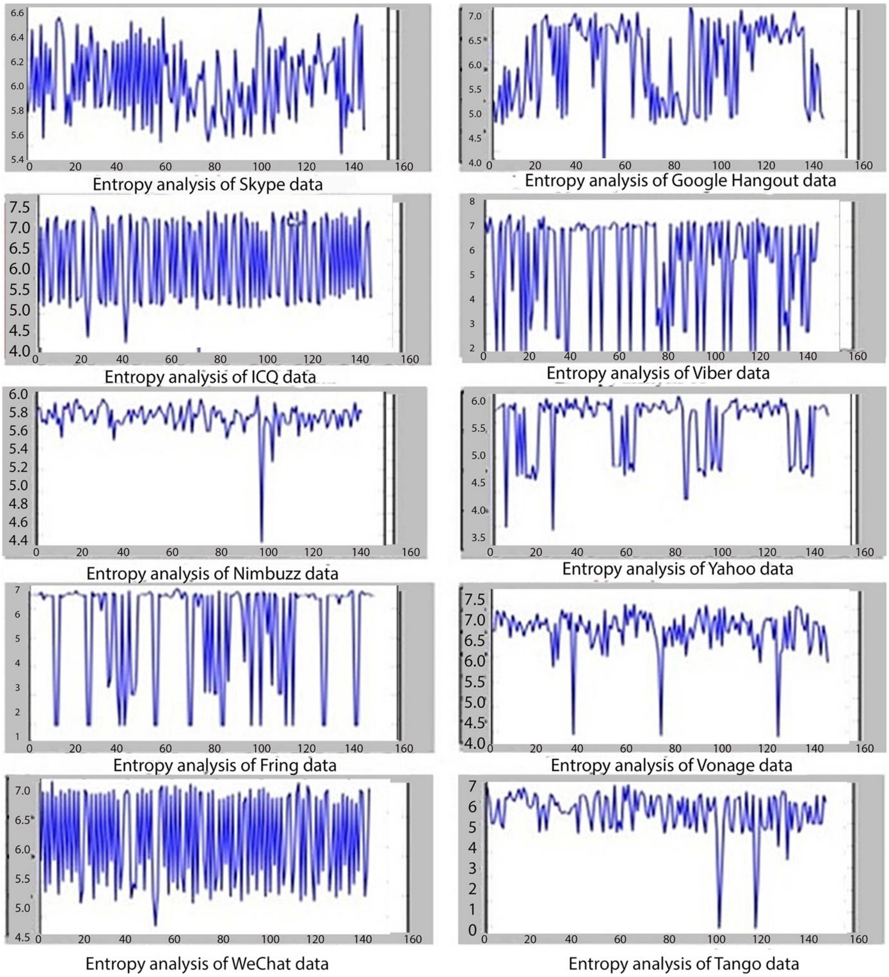
Histogram analysis of Fring data

Histogram analysis of Vonage data

Histogram analysis of WeChat data

Histogram analysis of Tango data

Fig. 16 Histogram analysis of w2m communications (sample 2)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

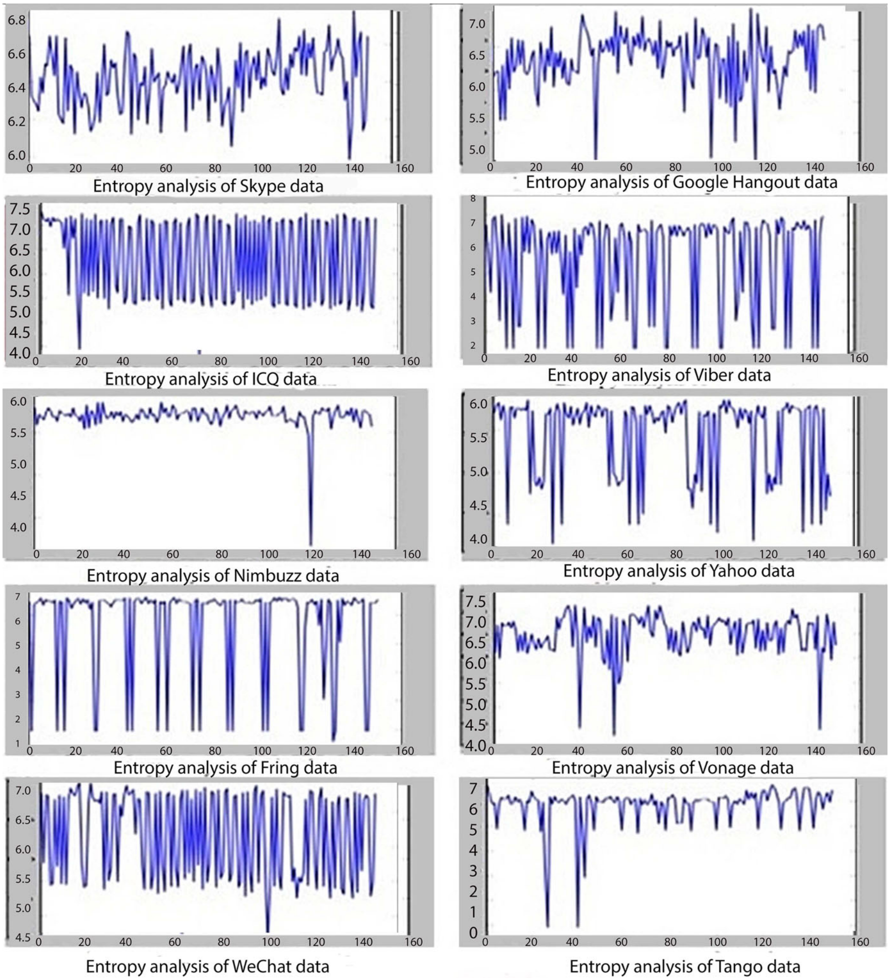
Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 17 Entropy analysis of w2m communications (sample 1)



Entropy analysis of Skype data

Entropy analysis of Google Hangout data

Entropy analysis of ICQ data

Entropy analysis of Viber data

Entropy analysis of Nimbuzz data

Entropy analysis of Yahoo data

Entropy analysis of Fring data

Entropy analysis of Vonage data

Entropy analysis of WeChat data

Entropy analysis of Tango data

Fig. 18 Entropy analysis of w2m communications (sample 2)

References

1. Appelman, M., Bosma, J., & Veerman, G. (2011). Viber communication security: Unscramble the scrambled.
2. Australian Government Department of Broadband Communications and Digital Economy. (2013). Statistical Snapshot.
3. Azab, A., Watters, P., & Layton, R. (2012). Characterising network traffic for skype forensics. In *Proceedings of the Third Cybercrime and Trustworthy Computing Workshop (CTC)*, Australia, 29–30 October 2012 (pp. 19–27).
4. Azfar, A., Choo, K.-K. R., & Liu, L. (2014). A study of ten popular android mobile voip applications: Are the communications encrypted? In *Proceedings of the 47th Anual Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 6–9 January 2014 (pp. 4858–4867).
5. BKAV Internet Security Corporation (2013). Critical flaw in Viber allows full access to Android Smartphones, bypassing lock screen. Accessed April 30, 2013, from http://www.bkav.com/top-news/-/view_content/content/46264/critical-flaw-in-viber-allows-full-access-to-android-smartphones-bypassing-lock-screen.
6. Blond, S. L., Zhang, C., Legout, A., Ross, K., & Dabbous, W. (2011). I know where you are and what you are sharing: exploiting P2P communications to invade users' privacy. In *Proceedings of the ACM Internet Measurement Conference (SIGCOMM 2011), Germany, 2–4 November 2011* (pp. 45–60).
7. Cagnina, M., & Poian, M. (2009). Beyond e-business models: The road to virtual worlds. *Electronic Commerce Research, 9*(1–2), 49–75.
8. Carpenter, M., & Wright, J. (2009). Advanced metering infrastructure attack methodology. http://inguardians.com/pubs/AMI_Attack_Methodology.pdf.
9. Chang, H. (2013). The security service rating design for IT convergence services. *Electronic Commerce Research, 13*(3), 317–328.
10. Chang, Y. F., Chen, C. S., & Zhou, H. (2009). Smart phone for mobile commerce. *Computer Standards & Interfaces, 31*(4), 740–747.
11. Chen, Q., Chen, H.-M., & Kazman, R. (2007). Investigating antecedents of technology acceptance of initial eCRM users beyond generation X and the role of self-construal. *Electronic Commerce Research, 7*(3–4), 315–339.
12. Choo, K. K. R. (2009). *Secure key establishment. Advances in information security* (Vol. 41). New York: Springer.
13. Choo, K.-K. R. (2014). Mobile cloud storage users. *IEEE Cloud Computing, 1*(3), 20–23.
14. Choo, K.-K. R., Smith, R. G., & McCusker, M. (2007). *Future directions in technology-enabled crime: 2007–2009*. Canberra: Australian Institute of Criminology.
15. Does Skype use encryption? Retrieved January 30, 2014, from https://support.skype.com/en/faq/FA31/does-skype-use-encryption.
16. Dorfinger, P., Panholzer, G., & John, W. (2011). Entropy estimation for real-time encrypted traffic identification (Short Paper). In J. Domingo-Pascual, Y. Shavitt, & S. Uhlig (Eds.), *Traffic monitoring and analysis* (Vol. 6613, pp. 164–171, Lecture Notes in Computer Science): Springer Berlin Heidelberg.
17. Fring. Retrieved January 27, 2014, from http://www.fring.com/.
18. Ghaemmaghami, H., Dean, D., Sridharan, S., & McCowan, I. (2010). Noise robust voice activity detection using normal probability testing and time-domain histogram analysis. In *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), USA, 14–19 March 2010* (pp. 4470–4473).
19. Goldreich, O. (2004). *Foundations of cryptography: Volume 2, basic applications*. Cambridge: Cambridge University Press.
20. Gomes, J., Inacio, P., Pereira, M., Freire, M., & Monteiro, P. (2013). Identification of peer-to-peer VoIP sessions using entropy and codec properties. *IEEE Transactions on Parallel and Distributed Systems, 24*(10), 2004–2014.
21. Google How Hangouts encrypts information. Retrieved April 3, 2015, from https://support.google.com/hangouts/answer/6046115?hl=en#.
22. Guo, J.-I., Yen, J.-C., & Pai, H.-F. (2002). New voice over Internet protocol technique with hierarchical data security protection. *IEE Proceedings: Vision, Image and Signal Processing, 149*(4), 237–243.
23. Hester, J. (2009). Big Blue Ball.com: Instant messaging & social networking. Accessed January 25, 2014, from http://www.bigblueball.com/im/googletalk/.

24. ICQ. (2011). ICQ Privacy Policy. Accessed April 3, 2015, from http://www.icq.com/legal/privacypolicy/en.
25. Infonetics Research raises VoLTE forecast; Over-the-top mobile VoIP subscribers nearing 1 billion mark (2013). Accessed January 15, 2014, from http://www.infonetics.com/pr/2013/Mobile-VoIP-Services-and-Subscribers-Market-Highlights.asp.
26. Jahanirad, M., AL-Nabhani, Y., & Noor, R. M. (2011). Security measures for VoIP application: A state of the art review. *Scientific Research and Essays, 6*(23), 4950–4959.
27. Johnson, M., Ishwar, P., Prabhakaran, V., Schonberg, D., & Ramchandran, K. (2004). On compressing encrypted data. *IEEE Transactions on Signal Processing, 52*(10), 2992–3006.
28. King, A., & Lyons, K. (2011). Automatic status updates in distributed software development. In *Proceedings of the 2nd International Workshop on Web 2.0 for Software Engineering, USA, 21–28 May 2011* (pp. 19–24).
29. Lee, J., Ko, H.-S., Park, S., Seo, M., & Kim, I. (2011) .Study on secure mobile communication based on the hardware security module. In *Fifth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2011), Portugal, 20–25 November 2011* (pp. 23–26)
30. Ludwig, S., Beda, J., Saint-Andre, P., McQueen, R., Egan, S., & Hildebrand, J. (2009). XEP-0166: Jingle. Accessed January 30, 2014, from http://xmpp.org/extensions/xep-0166.html.
31. Menghui, Y., Hua, L., & Tonghong, L. (2010). Implementation and performance for lawful intercept of VoIP calls based on SIP session border controller. In *Proceedings of the IEEE 10th International Conference on Computer and Information Technology (CIT), United Kingdom, 29 June-1 July 2010* (pp. 2635–2642).
32. Misra, S. K., & Wickamasinghe, N. (2004). Security of a mobile transaction: A trust model. *Electronic Commerce Research, 4*(4), 359–372.
33. Nimbuzz. Accessed January 30, 2014, from http://www.nimbuzz.com/en/support.
34. NSA slides explain the PRISM data-collection program. (2013). *The Washington Post.*
35. PcapHistogram. Retrieved January 30, 2014, from http://www.willhackforsushi.com/code/pcaphistogram.pl.
36. Perez, J. C. (2013, May 25). Google defends its use of proprietary tech in Hangouts. *PC World*
37. pyNetEntropy. Accessed January 30, 2014, from https://github.com/batidiane/pyNetEntropy.
38. Sarkar, A. (2012). Yahoo! Voice Compromised, 450 K Login Credentials Stolen & Posted In Plain Text. Accessed January 30, 2014, from http://www.voiceofgreyhat.com/2012/07/yahoo-voice-compromised-450k-login.html.
39. Shannon, C. E. (1951). Prediction and entropy of printed English. *Bell Systems Technical Journal, 30*(1), 50–64.
40. Shepard, B. (2013). 10 Cool Ways Companies Use Skype. Accessed January 30, 2014, from http://blogs.skype.com/2013/08/28/happy-10th-ten-cool-ways-companies-use-skype/.
41. Soupionis, Y., Basagiannis, S., Katsaros, P., & Gritzalis, D. (2011). A formally verified mechanism for countering SPIT. In C. Xenakis, & S. Wolthusen (Eds.), *Critical Information Infrastructures Security* (Vol. 6712, pp. 128–139, Lecture Notes in Computer Science): Springer Berlin Heidelberg.
42. Tango. Accessed January 27, 2014, from http://www.tango.me/.
43. Viber are my messages secure? Accessed April 3, 2015, from https://support.viber.com/customer/portal/articles/1600146-are-my-messages-secure-#.VR321vmUeSo.
44. Viber Connect Freely. Accessed January 15, 2015, from http://www.viber.com/.
45. VoIP Users Conference. Accessed January 27, 2014, from http://www.voipusersconference.org/2011/jabber-jitsi-nimbuzz/.
46. Vonage Mobile. Accessed January 30, 2014, from http://www.vonagemobile.com/.
47. Vrakas, N., & Lambrinoudakis, C. (2013). An intrusion detection and prevention system for IMs and VoIP services. *International Journal of Information Security, 2*(3), 201–217.
48. Wang, C.-H., & Liu, Y.-S. (2011). A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes. *Journal of Network and Computer Applications, 34*(5), 1545–1556.
49. WeChat The New Way to Connect. Accessed January 15, 2015, from http://www.wechat.com/en/.
50. Wright, C. V., Ballard, L., Monrose, F., & Masson, G. M. (2007). Language identification of encrypted VoIP traffic: Alejandra y Roberto or Alice and Bob? In *USENIX Security, 2007* (Vol. 3, pp. 43–54, Vol. 3.6)
51. Yahoo! 7 Messenger. Accessed January 30, 2014, from http://au.messenger.yahoo.com/features/.

Abdullah Azfar is a Ph.D. Scholar at the University of South Australia. He worked as an Assistant Professor in the Computer Science and Engineering Department of Islamic University of Technology (IUT), Bangladesh, after completing his master studies in Security and Mobile Computing from Norwegian University of Science and Technology (NTNU), Norway and The Royal Institute of Technology (KTH), Sweden in 2010. He received his bachelor degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2005. He is the recipient of Australian Postgraduate Award Scholarship (APA). He also received the Erasmus Mundus scholarship from the European Union for his master studies. His research interests are mainly focused on Android forensics, information systems, and VoIP communication security and privacy.

Kim-Kwang Raymond Choo is a Fulbright Scholar and Senior Researcher at the University of South Australia. He graduated with a Ph.D. in Information Security from Queensland University of Technology in 2006. He has co-edited a book entitled “Cloud Security Ecosystem” (Elsevier, 2015), and (co)authored two research books (Springer, 2008; Elsevier, 2014), seven Australian Government refereed monographs, 15 refereed book chapters, 77 refereed journal articles, 52 refereed conference articles and six parliamentary submissions. His research has been widely cited, including in key government reports by the Australian Government, United Nations Office on Drugs and Crime, and International Telecommunication Union. He is the Special Issue Guest Editor of IEEE Transactions on Cloud Computing “Cloud Security Engineering”, IEEE Cloud Computing “Legal Clouds”, Future Generation Computer Systems “Cloud Cryptography”, Journal of Computer and System Sciences “Cyber Security in the Critical Infrastructure”, Pervasive and Mobile Computing “Mobile Security, Privacy and Forensics”, Digital Investigation “Cloud Forensics”, ACM Transactions on Internet Technology “Internet of Things (IoT)”, ACM Transactions on Embedded Computing Systems “Embedded Device Forensics and Security”, and Multimedia Tools and Applications “Multimedia Social Network Security and Applications”. He is the recipient of several awards including a 2008 Australia Day Achievement Medallion in recognition of his dedication and contribution to the AIC, and through it to the public service of the nation, the British Computer Society’s Wilkes Award for the best paper published in the 2007 volume of the Computer Journal, and the Best Student Paper Award by the 2005 Australasian Conference on Information Security and Privacy. In 2009, he was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine/Microsoft’s Next 100 series.

Lin Liu is a Senior Lecturer at the School of IT and Mathematical Sciences, University of South Australia (UniSA). Dr Liu received her bachelor and master degrees in Electronic Engineering from Xidian University, China, and her Ph.D. degree in computer systems engineering from UniSA. Dr Liu’s research interests include Petri nets and their applications to protocol verification and network security analysis, as well as data mining and its applications to biological data analysis. She has published over 40 refereed journal and conference papers in the aforementioned research fields.