Social Networks IM Forensics: Encryption Analysis

Nedaa B. Al Barghuthi[1] and Huwida Said[2]
[1] Advanced Networks Security Research Laboratory, Electrical and Computer Engineering, College of Engineering, University of Sharjah, Sharjah 31286, UAE
[2] Advanced Cyber Forensics Research Laboratory, College of Technological Innovation, Zayed University, Dubai 19282, UAE
Email: nedaa@sharjah.ac.ae; huwida.said@zu.ac.ae

Abstract**—**In most regards, the twenty-first century may not bring revolutionary changes in electronic messaging technology in terms of applications or protocols. Security issues that have long been a concern in messaging application are finally being solved using a variety of products. Web-based messaging systems are rapidly evolving the text-based conversation. The users have the right to protect their privacy from the eavesdropper, or other parties which interferes the privacy of the users for such purpose. The chatters most probably use the instant messages to chat with others for personal issue; in which no one has the right eavesdrop the conversation channel and interfere this privacy. This is considered as a non-ethical manner and the privacy of the users should be protected. The author seeks to identify the security features for most public instant messaging services used over the internet and suggest some solutions in order to encrypt the instant messaging over the conversation channel. The aim of this research is to investigate through forensics and sniffing techniques, the possibilities of hiding communication using encryption to protect the integrity of messages exchanged. Authors used different tools and methods to run the investigations. Such tools include Wireshark packet sniffer, Forensics Tool Kit (FTK) and viaForensic mobile forensic toolkit. Finally, authors will report their findings on the level of security that encryption could provide to instant messaging services.

Index Terms— instant messages encryption; digital forensics; Andoird forensics; Yahoo; Google-Talk; Skype; Facebook; Whatsup; e-Buddyg; Gmail messenger; private web browsing.

I. Related Work

A. *Instant Messaging and Encryption*

Instant Messaging conversation is commonly used by wide range of Internet users. It can be recorded, monitored, and read [1]. Any data that travels over a network can be viewed using programs known as packet sniffers. These factors push clients to find a way for securing their IM conversation [2]. There are several ways to secure instant messaging and the most common used ways are web-based and the use of web applications. Web-based could be achieved through the use of private browsing mode while surfing the internet or chatting using instant messaging. On the other hand, many web applications provide a method of encryption to offer the required security level. Recently, instant messaging allow for the use of encrypted form of conversation. Most cryptographic algorithms provide a means for secret and authentic communication. According to [3], in 2011, a research paper proposed a secure module for the instant messaging which adds an additional “secure module” and apply a hash algorithm to encrypt the path between transceiver and routing modules as shown in Fig. 1 [3]. The most popular way to secure IM is by using encryption applications and using SSL feature in the internet browsers. Two basic encryption algorithms are available, the Symmetric and Asymmetric encryption algorithms [4], [5].

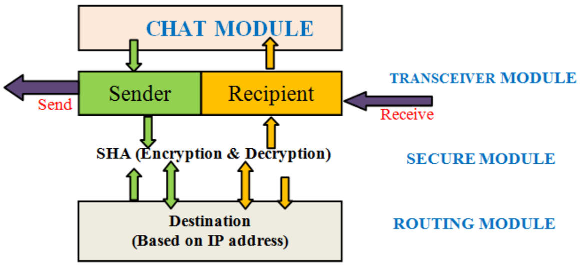


Figure 1. M. Yusof and A. Abidin proposed IM Secure Model [3]

In 2011, a research paper [6] discussed the basic requirements to have encryption in peer-to-peer social networks and proposed a method that combines two cryptography methods together (asymmetric and symmetric) to encrypt the communication channel. The proposed method does not have efficiency and functionality on the peer-to-peer social networks [6].

B. *Instant Messaging and Private Browsing Mode*

Private browsing modes can protect and hide the user’s identity over the internet, and attempts to look through their browsing history. It is designed to protect users from online tracking by third parties, from adversaries that access or control over the user's network and any a motivated attacker [7]. Private browsing prevents the storage of any information that identifies the user browsing habits.

1) *Google chrome private browsing mode (Incognito)*

Google Chrome offers the incognito browsing mode in which web pages that have been visited and files

Manuscript received June 15, 2013; revised September 30, 2013.
This work was supported by the Zayed University, Dubai, UAE Grant No.R12038.
Corresponding author email: nedaa@sharjah.ac.ae; huwida.said@zu.ac.ae
doi:10.12720/jcm.8.11.708-715

downloaded is not recorded in the browsing and downloads histories. All new cookies are deleted after closing all incognito windows, according to [8], [9] a research paper discussed the evidences left by private browsers sessions on a computer device.

2) Tor private browsing

Tor is a popular encryption tool which can be used in smart mobile device. It is designed to protect your anonymity over the internet and can encrypt your communications multiple times across the Internet [2]. According to [11], a research paper proposed a method to investigate a web browsing session artifacts left on Android mobile devices. It discussed the Tor browsing features and the proper method to acquire the digital smart device in order to retrieve all possible artifacts after browsing session.

C. Web-based Instant Messaging with SSL

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL encrypts the segments of network connections above the Transport Layer for key exchange, privacy, and message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, instant messaging and voice-over-IP (VoIP) [10].

D. Instant Messaging Applications and Encryption Tools

1) Skype instant messaging application:

Skype provides encrypted instant messages, video and voice connection via Internet (VoIP) which protects the clients from potential eavesdropping by malicious users. Skype uses the AES (Advanced Encryption Standard) and uses the maximum 256-bit encryption [12]. User public keys are certified by the Skype server at login using 1536 or 2048-bit RSA certificates [13]. According to [11], a research paper performed a network forensics on an encrypted communication channel and examined the artifacts left by Skype on the communication traffic.

2) Facebook instant messaging application

Facebook is one of the famous social website which has browsing security feature (https) in which the traffic becomes encrypted, making it harder for anyone else to access the Facebook information without permission [14]. Facebook encrypts the user’s information using secure socket layer technology (SSL). This may not always be apparent from the URL (web address), but rest assured our logins are secured [14]. According to [15], a research paper that performed a memory forensics on a live data acquisition within RAM of a desktop computer to investigate, analyze and collect a data related to Facebook artifacts on the device. In addition, a research paper [16] performed a physical acquisition to examine any artifacts left by Facebook on a computer device when using Arabic and Latin keywords in the text conversation.

3) Yahoo instant messaging application

In Yahoo! messenger the conversation messages are sent over the Internet in clear text form. According to [17], a research paper focused on YMSG protocol that used in Yahoo, examined the results and compared it with the other famous protocols. A recently added feature in Yahoo! Messenger allows users to connect with their Facebook friends through the messenger [18].

4) Google Talk instant messaging application

It is a web-based chatting host; the connection is encrypted between the Google Talk client and the Google Talk server, except when using Gmail's chat over HTTP. End-to-end messages are unencrypted. Google recently added encryption features for chat and call services. It is possible to have end-to-end encryption over the GTalk network using OTR (off-the-record) encryption [19].

5) eBuddy instant messaging application

It is a multi-protocol web-based instant messenger, offering support for Facebook, Gtalk, ICQ and Yahoo! Messengers [20].

6) Gmail web-based instant messaging application

Gmail is the first webmail provider to offer default HTTPS access. Though, the messages are encrypted over the transmission channel from your web browser to Google’s servers, which helps protect data from being attacked or manipulated by third parties if unsecured Internet connection is used [21].

7) Whatups instant messaging application

It is a mobile instant messaging application that personalized and decentralized, so that the message will be sent from end to end without passing any centralized servers through the communication channel [22].

8) SimpPro encryption application

The instant messages text in most of the applications is sent in clear text over the Internet, regardless of their destination. *SimpPro* secures popular instant messengers (e.g. Yahoo and Google Talk) by encrypting text messages and file transfers [23]. *SimpPro* is one of the tools that offered by a European company called Secway which created in early 2000 in France. The main SimpPro feature is to encrypt instant messages before they leave the sender’s computer [23]. Within SimpPro some symmetrical algorithms are available to encrypt your messages such as:

- AES (128 bits)
- 3DES (Tripe DES, 128 bits)
- CAST (128 bits)
- Twofish (128 bits)
- Serpent (128 bits) [23]

On the other hand asymmetrical algorithms are available for authentication and key agreement:

- RSA (2048 or 4096 bits)
- Diffie-Hellman
- ElGamal/DSA
- Elliptic curves [23]

Authentication keys are generated by SimpPro and cannot be reused in other encryption programs [23].

II. Research Objective

This paper analyzes the encryption level of the instant messenger in a laptop computer and smart mobile phones.

Instant messaging has become more popular that involve billions of users. The main goal of this paper is to investigate the encryption level of the instant message and seek a proper method to encrypt the conversation between two clients. Furthermore, the research is aimed to determine the possibilities of retrieving the encrypted conversation using sniffing and forensic tools. Many security enhancements have been proposed for instant messaging from the perspective of peer-to-peer communication. In addition, many instant messaging software with encryption features allow clients to encrypt their conversation and enhance the security level as well as maintaining efficiency and privacy in communication.

The research studies the existing encryption features of instant messaging. In, addition, the research paper investigates the techniques of hiding the communication between two parties using existing encryption to protect the integrity of the exchanged messages. This paper also evaluates the current implementation of instant messaging encryption by determining the encrypted conversation in smart mobile phones. Finally, the analysis to the encrypted messages was conducted using appropriate tools such as *SimpPro* and *Skype*.

III. Problem and Proposed Solution

A. *Hypothesis*

The authors aim is to encrypt instant messaging conversation and investigate the possibilities of retrieving the conversation text before and after applying the encryption. Authors also considered sniffing software and forensic tools to investigate the encryption algorithms. Mostly, the work is focus on making the instant messaging conversation more coded and difficult to predict. Further, the research initially specifies the research questions and scenarios as follows:

- How effective is the current implementation of encryption in Instant Messaging application on laptop computers and mobile smart phone devices?
- Ways to improve and strengthen encryption in Instant Messaging?
- What are the proper methods of encrypting any conversation text?
- How secure is the smart mobile phone IM over the laptop computer when encrypting any conversation text?

There are two approaches in this research paper, one is to encrypt Instant Messaging conversation text and investigate the security weaknesses in the encryption algorithm. The second is to investigate how to make Instant Messaging conversation coded.

IV. Research Methodology

To address the research questions, an experiment was implemented on how to encrypt the instant messaging and the possibilities to retrieve any evidence related to the conversation text message from windows laptops and android smart mobile phones.

A. *Instruments*

The following instruments were used in our experiment:

- Laptop PC running Windows 7 SP3 tested device
- Samsung Galaxy S3 smart phone tested device
- Tor Orweb v2.28 Android private browser app
- FTK forensic tool v.3.0
- FTK imager v.3.0
- Wireshark application installed on the forensic workstation
- viaForensics v5.5.2.1 installed on the forensic workstation
- Micro USB cable to connect the forensics workstation to the smartphone
- SimpPro to be installed on tested laptop
- Skype, Facebook, Yahoo and WhatsUp applications for tested devices

B. *Procedure*

The experiment consisted of Google Incognito private browsing session on Windows laptop and Tor private browsing session on Android smart mobile phone, followed by three forensic analyses – physical acquisition on the laptop device, live and logical analysis on the smart phone device.

1) *Usage scenario*

The work is started by identifying the encryption feature of the instant messengers on the tested devices. First, the authors installed the messengers and then performed chat conversation as follows:

Messenger	Test message
Skype Online Messenger	“Good morning”
Yahoo Online Messenger	“understand”
Facebook Online messenger	“my dear”
WhatsUp Online messenger	“hi”
eBuddy Web-based messenger	“How are you”
Gmail Chat Web-based messenger	“Mar7aba”
Google-Talk Web-based messenger	“School”
Facebook Web-base messenger	“University”

In order to encrypt the communication traffic, the authors defined a web client hosting SSL through Google private (incognito) browser and install SimpPro encryption tool on the tested device to encrypt the instant messaging between the peers.

The authors will analyze how strong the current implementation of encryption algorithms to instant messaging.

The authors repeated this experiment on a Galaxy S3 Android smart mobile device. Tor private browser is used to conduct the instant messaging as described in the above table.

- Finally findings and recommendations are reported.

2) *Examination of laptop device*

Two examinations were performed on the tested device. First, alive analysis is attempted via Wireshark sniffing tool to capture the communication traffic between peers and analyze the captured packets - Wireshark is an open source software project, and is released under the GNU General Public License. It is a network packet analyzer which tries to capture network packets and tries to display that packet data as detailed as possible [24].

After that, a physical acquisition was performed on the hard disk of the device via FTK imager. FTK forensic tool was used to analyze the acquired forensic image of the test device to investigate the possibilities to retrieve the conversation text. This process is repeated twice, before and after the encryption process over the communication channel between the peer.

3) *Examination of android mobile device*

A logical acquisition was attempted on Android mobile device. First, the authors installed viaForensic utility on the forensic workstation - viaForensic is a forensic utility, very useful for android logical acquisition without the need to root the device. Steve Kovacik discussed in his research a proposed methodology for using this utility in an effectiveness way [25].

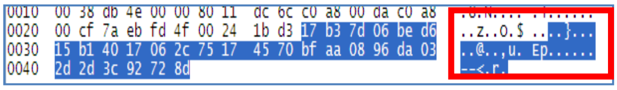
Then, the smart phone is connected via a USB cable to the forensic workstation. After that, a logical acquisition was performed on the device. Android provides a relationship database for each application using SQLlite database viewer to store data securely and efficiently. The acquired image was analyzed through viaForensics utility and SQLite database viewer and investigates any evidence related to the instant messaging.

V. Results

A. *Laptop Computer Device*

1) *Skype instant messaging application*

The Skype engine encrypts the instant message by default without needs for encryption tools shown in Fig. 2. According to [28], a research paper focused on a selective algorithm that implemented on Skype client. The result matches with the result of this section.

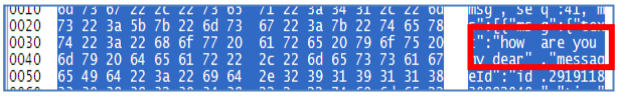


```
0020  00 cf 7a eb fd 4f 00 24  1b d3 17 b3 7d 06 be d6   ..z..O.$ ....}...
0030  15 b1 40 17 06 2c 75 17  45 70 bf aa 08 96 da 03   ..@..,u. Ep......
0040  2d 2d 3c 92 72 8d                                   --<.r.
```

Figure 2. IM is encrypted in skype messenger

2) *Facebook instant messaging application*

Identifying the encryption feature in Facebook web-based messenger using Wireshark packet sniffer shown in Fig. 3.



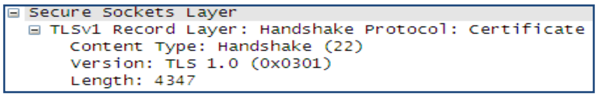
```
0020  73 22 3a 5b 7b 22 6d 73  67 22 3a 7b 22 74 65 78
0030  74 22 3a 22 68 6f 77 20  61 72 65 20 79 6f 75 20   t":"how  are you
0040  6d 79 20 64 65 61 72 22  2c 22 6d 65 73 73 61 67   my dear" ,"messag
0050  65 49 64 22 3a 22 69 64  2e 32 39 31 39 31 31 38   eId":"id .2919118
```

Figure 3. Facebook plaintext captured by Wireshark

According to [15], a research paper discussed the Facebook artifacts on a desktop computer; it concluded that IM in Facebook is sent in plaintext, not encrypted nor encoded which matches the result of this section.

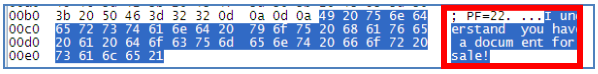
3) *Yahoo instant messenger application*

Encryption is implemented on Yahoo messenger using SimpPro encrypting tool as shown in Fig. 4, Fig. 5 and Fig. 6.



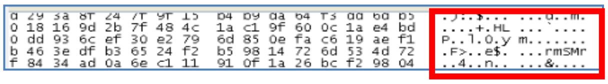
```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 4347
```

Figure 4. SimpPro enables SSL to secure the conversation channel



```
00b0  3b 20 50 46 3d 32 32 0d  0a 0d 0a 49 20 75 6e 64   ; PF=22. ...I und
00c0  65 72 73 74 61 6e 64 20  79 6f 75 20 68 61 76 65   erstand  you have
00d0  20 61 20 64 6f 63 75 6d  65 6e 74 20 66 6f 72 20    a docum ent for
00e0  73 61 6c 65 21                                      sale!
```

Figure 5. Yahoo plaintext before encryption capture by wireshark



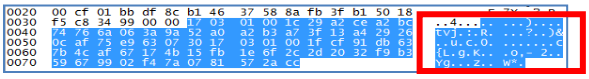
```
0 18 16 9d 2b 7f 48 4c  1a c1 9f 60 0c 1a e4 bd   ....+.HL ...`....
0 dd 93 6c ef 30 e2 79  6d 85 0e fa c6 19 ae f1   P..l.0.y m.......
b 46 3e df b3 65 24 f2  b5 98 14 72 6d 53 4d 72   .F>..e$. ...rmSMr
f 84 34 ad 0a 6e c1 11  91 0f 1a 26 bc f2 98 04   ..4..n.. ...&....
```

Figure 6. Yahoo encrypted message after using SimpPro captured by wireshark

According to [18], a research paper discussed YMGS protocol which used in Yahoo and explored that the message is sent over the channel is in plain text.which matched the result of this section.

4) *Gmail web-based IM messenger*

The Gmail chat encrypts the instant message by default without needs for encryption tools shown in Fig. 7.

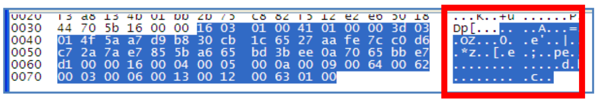


```
0020  00 cf 01 bb df 8c b1 46  37 58 8a fb 3f b1 50 18
0030  f5 c8 34 99 00 00 17 03  01 00 1c 29 a2 ce a2 bc   ..4..... ...)....
0040  74 76 6a 06 3a 9a 52 a0  a2 b3 a7 3f 13 a4 29 26   tvj.:.R. ...?..)&
0050  0c af 75 e9 63 07 30 17  03 01 00 1f cf 91 db 63   ..u.c.0. .......c
0060  7b 4c af 67 17 4b 15 fb  1e 6f 2c 2d 20 32 f9 b3   {L.g.K.. .o,- 2..
0070  59 67 99 02 f4 7a 07 81  57 2a cc                  Yg...z.. W*.
```

Figure 7. Gmail web-based IM messengers send IM in encrypted format through a secure socket layer

5) *Google Talk Web-based messenger*

The Google talk mail encrypts the instant message by default without needs for encryption tools shown in figure 8.

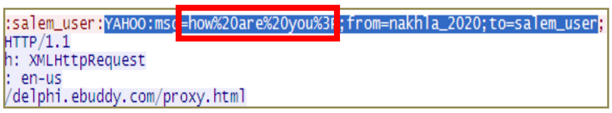


```
0030  44 70 5b 16 00 00 16 03  01 00 41 01 00 00 3d 03   Dp[..... ..A...=.
0040  01 4f 5a a7 d9 b8 30 cb  1c 65 27 aa fe 7c c0 d6   .OZ...0. .e'..|..
0050  c7 2a 7a e7 85 5b a6 65  bd 3b ee 0a 70 65 bb e7   .*z..[.e .;..pe..
0060  d1 00 00 16 00 04 00 05  00 0a 00 09 00 64 00 62   ........ .....d.b
0070  00 03 00 06 00 13 00 12  00 63 01 00               ........ .c..
```

Figure 8.SSL algorithm features to encrypt IM message in Google-Talk web-based messenger

6) *e-Buddy instant messaging application*

Identifying the encryption feature in e-Buddy web-based messenger using Wireshark packet sniffer shown in figure 9.



```
:salem_user:YAHOO:msg=how%20are%20you%3F;from=nakhla_2020;to=salem_user;
HTTP/1.1
h: XMLHttpRequest
: en-us
/delphi.ebuddy.com/proxy.html
```

Figure 9. eBuddy sends IM in plaintext captured by Wireshark

B. *Galaxy S3 Smart Mobile Device*

The authors used viaForensics utility in order to perform a logical acquisition of non-rooted smart mobile device and to access to the content of its databases through the SQLite Database Viewer- as shown in Table I. We are able to examine the content of database of each messenger- as shown in Table II.

TABLE I. MESSENGERS DATABASE LOCATIONS CAPTURED BY VIAFORENSICS UTILITY ON GALAXY S3 MOBILE DEVICE

Messenger	Artifact path location on the mobile device
Facebook via Orweb browser	"/data/data/info.guardianproject.browser/databases/ webview.db"
Facebook App.	"/data/data/com.facebook.orca/databases/thread_db 2"
Whatsup App.	"/data/data/com.whatsapp/databases/msgstore.db"
Skype App.	"/data/data/com.skype.reader"
Google-talk App.	"/data/data/com.google.android.talk"

VI. FINDINGS AND DISCUSSION

Data were analyzed and findings were presented satisfying the major research questions in this work, as follows:

- The author was able to identify the encryption algorithms used in the encryption tool to encrypt the instant message through the Wireshark packet sniffer and forensics investigating tools.
- The author identifies the encryption features using Wireshark packet sniffer at different instant messaging messengers and find results of laptop computer artifacts shown in Table III and results of Galaxy S3 smart mobile phone artifacts shown in Table IV.

TABLE II. SUMMARY OF INSTANT MESSAGING ARTICATS ON GALAXY S3

Messenger Description	Text conversation before encryption	Text conversation after encryption
Skype App.	1@16@a//13831837 …. (truncated)	1@16@a//13831837 …. (truncated)
Whatsp App.	"Hi"	-
Yahoo App.	"Understand"	8cg5vo57vlkpr!b=3&s ….. (truncated)
Gmail Web-based Messenger	ftP6T$vkFWLAHK ….. (truncated)	ftP6T$vkFWLAHKbt … (truncated)
Facebook Web-based Messenger	"University"	Rg4YPCLBvzhbUFZ …… (truncated)
Google-Talk Web-based Messenger	"School"	Aa74iu9OFHrsdYZB …… (truncated)

TABLE III. SUMMARY OF INSTANT MESSAGING ENCRYPTING WEB-BASED AND PEER-TO-PEER MESSENGERS ON LAPTOP COMPUTER

Messenger	Text conversation sent over internet	Text conversation after encryption	Text conversation after enabling SSL in Google (incognito) browser
Skype App.	Encrypted message	Encrypted message	-
Facebook Web-based	Plain text	-	Encrypted message
Gmail Web-based Messenger	Encrypted message	-	Encrypted message
Yahoo Web-based Messenger	Encrypted message	Encrypted message	-
eBuddy Web-based Messenger	Plain text	-	Plain text
Google-Talk Web-based Messenger	Plain text	-	Encrypted message

TABLE IV. SUMMARY OF INSTANT MESSAGING ENCRYPTING WEB BASED AND PEER-TO-PEER MESSENGERS ON GALAXY S3

Messenger	Text conversation format sent over internet	Text conversation using normal browser of Android	Text conversation (SSL is enabled in Orweb Private browser)
Skype App.	Encrypted message	-	-
WhatsUp App.	Plain text	-	-
Yahoo App.	Plain text	Encrypted message	-
Gmail Web-based Messenger	Encrypted message	-	Encrypted message
Facebook Web-based Messenger	Plain text	-	Encrypted message
Google-Talk Web-based Messenger	Plain text	-	Encrypted message

- The Trust level is an indicator that may be set manually by the user when he/she has to verify the identity of his/her contact. Typically, when receiving a new key from a contact, users are asked to accept or reject the key. In case of accepting it, the key is inserted in your keying and marked as un-trusted. Mainly, users may then verify the key by comparing its SHA hash with the SHA hash given by the real contact [26]. Once you have verified this, you may set the trust level to "Trusted", however, it is not automated since automating the key verification process would require setting up global PKI (public key infrastructure). The "Trust level" is a convenient alternative to PKI systems [23].

- SimpPro encrypts private keys with the password and a symmetrical algorithm, such as AES or Twofish. This ensures that the private key is not accessible, even if the computer is stolen [23].
- To get a security feature, the user should require using a browser that supports 128-bit SSL. It enables the browser to provide a secure connection with a secure Web server.
- The author uses encryption tool (SimpPro) to encrypt the text conversation in online messenger applications and finds that Yahoo Messenger sent the conversation text in encrypted format.
- The author finds that the encrypting tool SimpPro has a strong algorithm that mix between asymmetric and symmetric encryption methods.
- To get a security feature, the user should require using a browser that supports 128-bit SSL (Secure Socket Layer) encryption. It enables the browser to provide a secure connection with the secure Web server. The authors enabled the SSL feature in Google Chrome (incognito mode) and Orweb private browser. The following is their result:
    - Skype peer-to-peer instant messenger provide the best security level compared to other peer-to-peer IM.
    - Google-Talk web-based instant messenger sent encrypted text messages.
    - Facebook web-based instant messenger sent the text conversation in encrypted text through Orweb private browser.
    - Gmail web-based instant messenger provide the best security level compared to other web-based IM.

VII. Research Challenges

The researchers faced many difficulties and challenges in investigating the implementation for the instant message as follows:

- When using the web-based messengers, there were some online messengers that lack of secure protocol (i.e https) at their server such as Google-Talk web-base site. To improve secure communication the author enables SSL feature on the Google incognito browser, to show the encrypted messages appear over the channel.
- Yahoo messenger is not supporting encryption within the messenger; as a result the author has to use an open source tool (i.e SimpPro) to encrypt the conversation channel.
- However, this solution is not applied when used in Facebook web-based messenger and eBuddy web-based messenger, as a solution, the author suggests to use a VPN proxy server and create a VPN connection at the client side to access to the web-based messenger through a secure channel.

The Wireshark packet sniffer tool is not supporting the instant messaging file transfer, and due to the limited time, the author tries to comparing, investigate and implement encrypting feature in the most messengers used over the internet and suggest security enhancement to them in order to insure privacy to the users.

VIII. Conclusion and Future Work

In order to enhance the security features and have a secure conversation channel between the chatters, it is required to have a security feature in a messaging system consists of different requirements such as user identification, access and authentication to the network and messaging system. Also, there is the encryption and message authenticity (digital signature) to be added to the message.

The users have the right to protect their privacy from the eavesdropping attackers, or other parties which interferes the privacy of the users. The chatters most probably use the instant messages to chat with others; this is considered as privacy issues in which no one has the right to eavesdrop the conversation channel. This is considered as a non ethical manner and the privacy of the user should be protected.

As a future work, the author intended to study the encryption feature in iMessage application on Android which launched recently, and investigate the possibilities to encrypt a file and transfer it over the conversation channel and examine the possibilities to secure the encrypted file.

The author recommends some steps that the users should do before using any instant messaging tool in order to protect their conversation privacy:

- Ensure that the internet and www-based application are protected by using SSL feature in the browser and https feature is available at the web-host server.
- If the browser is not supporting the SSL feature then the user may use a VPN connection in order to connect to a SSL proxy server through the internet.
- An SSL VPN (Secure Sockets Layer virtual private network) can be used with a standard Web browsing. It can also give remote users an access to Web applications, client/server applications and internal network connections [27].
- The users may use enhanced encrypted tools to encrypt the instant messages to the other party.

Instant Messaging can be secured in many different ways to be protected against keystroke capturing and monitoring software. Instant messaging also involves set of best practices to ensure the data protection. Instant messaging (IM) can be secured using IM encryption software and tools that are widely available and easy to download. Using Instant Messaging applications in the private browsing mode will also provide good level of security to the IM conversation data. Furthermore, SSL can provide a secure channel for online conversation. IM security in corporate network should involve establishment of an IM usage policy and properly configure perimeter firewalls to block all non-approved instant messaging and transferred files [3].

The following is suggested by author to enhance the security feature in instant messaging through software developing:

- The message can be encrypted and digitally signed so that if a message is intercepted during the transmission, it cannot be read or modified without detection.
- When a message is encrypted, typically the sender of the message applies the encryption using a private key, which can then only be decoded by the recipient with the originator's public key.
- In addition to encryption, a message can be signed using similar key pair and the signature of the message. If the message is somehow changed during the transmission, the signature will not match when decoded by the recipient.
- A security system can be used to manage the keys within the messaging system.

REFERENCES

[1] Instant Messaging homepage on TechTarget website. (2008). [Online]. Available: http://searchunifiedcommunications.techtarget.com/definition/instant-messaging

[2] (N.A). Instant Messaging homepage on Surveillance Self-Defense website. [Online]. Available: https://ssd.eff.org/tech/im

[3] M. Yusof and A. Abidin, "A secure private instant messenger," in *Proc. 17th Ascia-Pacific Conference on Communications*, 2011, pp. 821-825.

[4] Ayushi, "A symmetric key cryptographic algorithm," *International Journal of Computer Applications*, vol. 1, no. 15, 2010.

[5] What is public-key cryptography homepage on RSA Laboratories. (2012). [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2165

[6] O. Bodriagov and S. Buchegger, "Encryption for Peer-to-Peer social networks," in *Proc. IEEE Conference on Privacy, Security and Trust, and IEEE Conference on Social Computing*, 2011, pp. 1302-1309.

[7] C. Soghoian, "Why private browsing modes do not deliver real privacy," *Center for Applied Cybersecurity Research*, Indiana University, 2011.

[8] Saad Hamid. (2008). Enable private browsing mode in Google Chrome. [Online]. Available: http://www.sizlopedia.com/2008/09/03/enable-private-browsing-mode-in google-chrome/

[9] N. AlMutawa, H. Said, I. AlAwadi and M. Guirmaraes, "Forensic Analysis of private browsing artifacts," in *Proc. 7th International Conference on Innovation in Information Technology*, 2011.

[10] OWASP. Transport Layer Protection Cheat Sheet. (2013). [Online]. Available: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

[11] N. Al Barghouthi, A. Marrington, and I. Baggali, "The forensic investigation of android private browsing sessions using orweb," in *Proc. 5th International Conference on CSIT*, 2013.

[12] C. Leung and Y. Chan, "Network forensics on encrypted Peer-to-Peer VoIP traffics and the detection, blocking and prioritization of skype traffics," in *Proc. 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2007.

[13] Skype website. (2012). [Online]. Available:http://www.skype.com

[14] Facebook website. (2012). [Online]. Available: http://www.facebook.com/help/search/?q=encryption

[15] H. Chu, D. Deng, and J. Part, "Live data mining concerning social networking forensics based on a facebook session through aggregation of social data," *IEEE Journal on Selected Areas in Communications*, vol.29, no. 7, Auguest 2011.

[16] I. Alwadi, I. Baggil, and A. Marrington, "Forensic artifacts of facebook's instant messaging service," in *Proc. International Conference for Internet Technology and Secured Transactions*, 2011.

[17] Time van Lokven. Review and Comparison of instant messaging protocols. (2011). [Online]. Available: http://www.cs.ru.nl/bachelorscripties/2011/Tim_van_Lokven___0438006___Review_and_Comparison_of_Instant_Messaging_Protocols.pdf

[18] (N.A). Yahoo messenger homepage on Yahoo! Messenger website. [Online]. Available: http://messenger.yahoo.com/

[19] Google Talk Channel homepage on IFTTT website. (2013). [Online]. Available: https://ifttt.com/google_talk

[20] CrunshBase homepage on eBuddy website. (2013). [Online]. Available: http://www.crunchbase.com/company/ebuddy

[21] Google website. (2012). [Online]. Available: http://support.google.com/mail/bin/answer.py?hl=en&answer=1304609

[22] Boutet, D. Frey, R. Guerraoui, and A. Kermarrec, "Whatsup: News, From, For, Through, Everyone," *IEEE P2P*, 2010.

[23] Secway website. (2011). [Online]. Available:http://www.secway.fr/

[24] Wireshark website. (2009). [Online]. Available: http://www.wireshark.com

[25] S. Liles, S. Kovacik, and D. O'Day. Proposed Methodology for Victim Android Forensics. (2010). [Online]. Available: Proposed-Methodology-for-Android-Forensics.pdf

[26] (N.A). Securing Instant Messaging homepage one Symantic website. [Online]. Available: http://www.symantec.com/avcenter/reference/secure.instant.messaging.pdf

[27] SSL VPN (Secure Sockets Layer virtual private network) homepage on Search Security website. (2006). [Online]. Available: http://searchsecurity.techtarget.com/definition/SSL-VPN

[28] A. Ramdan and R. Munir, "Selective encryption algorithm implementation for video call on skype client," in *Proc. 7th International Conference on Telecommunication Systems, Services and Applications*, 2012.

Nedaa Baker Al Barghuthi is a Network Security Engineer in the College of Engineering at University of Sharjah, Sharjah, UAE. She received her Bachelor of Engineering (B.Eng.) in Electronics and Communication Engineering from the Applied Science University, Amman, Jordan and M.Sc. (Distinguish with Honors) in Cyber Security from Zayed University, Dubai, UAE. Al Barghuthi's teaching interests are computer information security, network and internet security. Her research interests include cyber forensics, mobile forensics, information security, computer networking, internet security, digital forensics, small scale digital forensics, database systems and security. She has published several conference papers in small scale digital devices forensics. She has published several peer-reviewed papers in journals and conferences.

Huwida Said is an Associate Professor in the College Technological Innovation at Zayed University, Dubai, UAE. She received her Bachelor of Engineering (B.Eng.) in Electrical and Electronics Engineering from the University of Wales Swansea, UK, and a Ph.D. in Computer Sciences from the University of Reading, UK, in 1999. In 2008, she received a fellowship to conduct a post-doctorate certificate in information assurance from the University of Maryland University College UMUC, Maryland USA. Her teaching interests are computer information security, network and internet security. Her research interests include information security, computer networking, internet security, video game to teach information security, database systems computer forensics and mobile forensics She has published several peer-reviewed papers in journals and conferences, and she is the founder and co-chair of the Undergraduate Intercollegiate Cyber Defense Competition (UICDC) in the UAE and the GCC area since 2011.