Avrupa Bilim ve Teknoloji Dergisi
Cilt. 2, No. 4, S. 112-117, Haziran 2015
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Vol. 2, No. 4, pp. 112-117, June 2015
Copyright © 2014 EJOSAT
Research Article

Survey of Instant Messaging Applications Encryption Methods

Abdullah Talha Kabakus[1*], Resul Kara[2]

[1] Abant Izzet Baysal University, IT Center, 14280, Bolu, Turkey
[2] Duzce University, Faculty of Engineering, Department of Computer Engineering, 81620, Duzce, Turkey

(First received 15 February 2015 and in final form 29 May 2015)

Abstract

Instant messaging applications has already taken the place of traditional Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) due to their popularity and usage easement they provide. Users of instant messaging applications are able to send both text and audio messages, different types of attachments such as photos, videos, and contact information to their contacts in real time. Because of instant messaging applications use internet instead of Short Message Service Technical Realization (GSM), they are free to use and they only require internet connection which is the most common way of communication today. The critical point here is providing privacy of these messages in order to prevent any vulnerable points for hackers and cyber criminals. According to the latest research by PricewaterhouseCoopers, percentage of global cyber attacks is increased to 48% with 42.8 million detected incidents. Another report that is published by security company Postini indicates that 90% of instant messaging targeted threats are highly destructive worms. In this study, instant messaging applications encryption methods are comparatively presented. Instant messaging applications are investigated considering three different target platforms: (1) Desktop clients, (2) web clients, and (3) mobile phone clients. Instant messaging applications are compared through the critical criteria that most research studies emphasize: (1) Text conversation over internet, (2) text conversation after encryption, and (3) text conversation after enabling Secure Sockets Layer (SSL). Finally, authors highlight key requirements of a secure instant messaging application should provide.

Keywords: Instant messaging, digital forensics, message encryption, mobile security

Özet

Anlık mesajlaşma uygulamaları, kolay kullanımları ve popülaritelerinden dolayı geleneksel Kısa Mesajlaşma Servisi (SMS) ve Çoklu Medya Mesajlaşma Servisi (MMS)'in yerini aldı. Anlık mesajlaşma uygulama kullanıcıları, bu uygulamalar aracılığıyla metin, ses mesajları, fotoğraf, video, kişi bilgisi gibi çeşitli türlerdeki ekleri arkadaşlarıyla gerçek zamanlı olarak paylaşabilmektedir. Anlık mesajlaşma uygulamaları Kısa Mesaj Servisi Teknik Gerçeklemesi (GSM) yerine sadece günümüzde en çok kullanılan iletişim aracı olan internete ihtiyaç duyduğundan dolayı ücretsizdir. Buradaki kritik nokta, siber saldırganlarına ve bilgisayar korsanlarına karşı herhangi açık nokta bırakmamak için bu mesajların güvenliğinin sağlanmasıdır. PricewaterhouseCoopers tarafından yapılan son rapora göre, 2014 yılında tespit edilen uluslararası siber saldırılar sayısı 42.8 milyona çıkarak %48'e yükselmiştir. Postini güvenlik şirketi tarafından yayınlanan başka bir rapor ise anlık mesajlaşmayı hedefleyen tehditlerin %90'ının oldukça yıkıcı solucanlar olduğunu belirtmektedir. Bu çalışmada, anlık mesajlaşma uygulamalarının şifreleme yöntemleri karşılaştırmalı olarak sunulmuştur. Anlık mesajlaşma uygulamaları üç farklı platform göz önüne alınarak incelenmiştir: (1) Masaüstü istemcileri, (2) web istemcileri ve (3) mobil telefon istemcileri. Anlık mesajlaşma uygulamaları, birçok araştırmada en çok üzerinde durulan kritik kriterler olan (1) internet üzerinden metin dönüşümü, (2) şifreleme sonrası metin dönüşümü ve (3) Güvenli Giriş Katmanı (SSL) kullanıldıktan sonra yapılan metin dönüşümüne göre karşılaştırılmıştır. Son olarak yazarlar, güvenli bir mesajlaşma uygulamasında bulunması gereken kritik gereksinimleri vurgulamıştır.

Anahtar Kelimeler: Anlık mesajlaşma, adli bilişim, mesaj şifreleme, mobil güvenlik

1. Introduction

Instant messaging applications let users to send both text and audio messages, different types of attachments such as photos, videos and contact information in real time. Most of instant messaging applications provide two types of communication: (1) peer-to-peer, (2) group chat. Advantages of instant messaging applications can be listed as: (1) They are free and just require internet connection, (2) there is no restriction on the length or the number of messages, (3) they automatically import contacts on mobile phone or another service they support, and (4) they provide users to create richer profiles. Instant messaging applications always top download lists for different platforms. For example, WhatsApp[1] –a cross-platform instant messaging application acquired by Facebook[2] - is currently *(January 2015)* the most popular third application on Google Play Store[3] – the

[*] Abdullah Talha Kabakus, E-posta: talha.kabakus@ibu.edu.tr, Tel.: 0374 254 10 00 / 1807, Fax: 0374 253 45 26

[1] http://www.whatsapp.com

[2] https://www.facebook.com

[3] https://play.google.com/store

official application market for Android. According to the recent report of Technoduce[4], WhatsApp is the most popular instant messaging application with 450 million active monthly users (“Infographic Top 10 Most Popular Instant Messaging Apps In The World,” 2014). Similarly, Facebook Messenger – official messenger application of Facebook - is the most popular second application on Google Play Store with more than 500 million downloads as January 2015. The key reason behind this popularity is that instant messaging applications use internet instead of Short Message Service Technical Realization (GSM), they are free to use and they only require internet connection which is the most common way of communication today. According to the latest research by PricewaterhouseCoopers (“Global Information Security Survey: 2015 Results by Industry,” 2015), average of global cyber attacks is increased to 48% with 42.8 million detected incidents. According to a recent report by security company *Postini*[5] (“Instant messaging targeted for malicious worm attack,” 2006), instant messaging threats are increased by 1700% in 2005 and 90% of these threats are highly destructive worms. According to Sanchez J. (Sanchez, 2014), most of these highly-popular instant messaging applications including WhatsApp have some known vulnerabilities.

Yusof and Abidin (Yusof and Abidin, 2011) propose a secure model for instant messaging by adding additional “secure model” and apply a hash algorithm to encrypt the path between transceiver and routing modules as it is shown in Fig. 1.

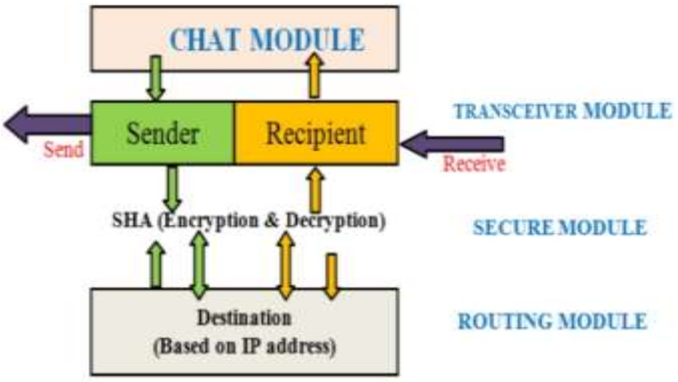


Fig. 1. *Proposed instant messaging secure model by Yusof and Abidin (Yusof and Abidin, 2011)*

Bodriagov and Buchegger (Bodriagov and Buchegger, 2011) propose a new approach that combines asymmetric and symmetric cryptography methods to encrypt the communication channel. The proposed method does not have sufficient efficiency and functionality for peer-to-peer social networks.

The paper is structured as follows: In section 2, encryption tools that are used by different encryption methods are presented. In section 3, instant messaging applications encryption methods are presented. Section 4 presents results and discussion. Finally, section 5 concludes the paper.

2. Encryption Tools

In this section, encryption tools such as Simp, DB Browser for SQLite that are commonly used by different encryption methods are presented.

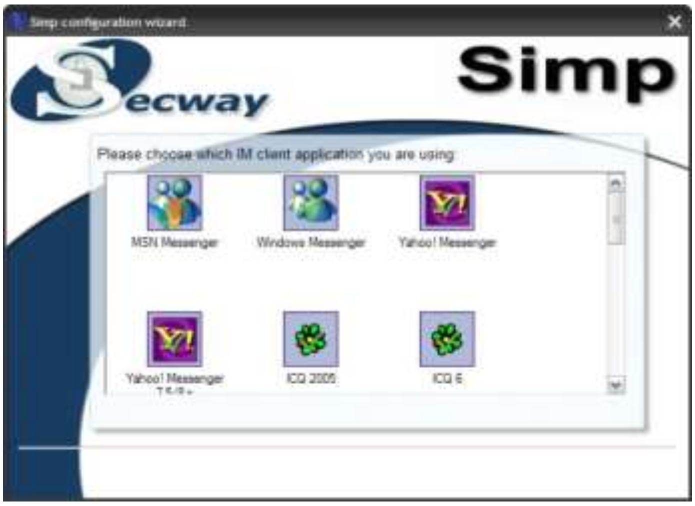
2.1. Simp

Simp[6] secures popular instant messengers such as Google Talk, Yahoo, ICQ, AIM, MSN Messenger by encrypting text messages and file transfers (“Secway,” n.d.). Simp can also encrypt instant messages before they leave the client (“Secway,” n.d.). Simp's configuration wizard user interface to select instant messaging applications is presented in Fig. 2. Symmetrical algorithms provided by Simp to encrypt messages can be listed as (Barghuthi and Said, 2013):

- AES (128 bits)
- 3DES (Triple DES, 128 bits)
- CAST (128 bits)
- Twofish (128 bits)
- Serpent (128 bits)

Simp provides asymmetrical algorithms for authentication and key agreement such as (Barghuthi and Said, 2013):

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



Please choose which IM client application you are using

Fig. 2. Simp's configuration wizard user interface

Simp encrypts private keys with a password and a symmetrical algorithm. Hence, the private key is not accessible even the data is stolen (“Secway,” n.d.).

2.2. DB Browser for SQLite

DB Browser for SQLite[7] is an open-source cross-platform tool to create, design and edit database files compatible with SQLite[8] (“DB Browser for SQLite,” n.d.). SQLite is a powerful, embedded relational database management system in a compact C library (Owens, 2003). SQLite databases are commonly used by mobile applications to store their artifacts such as message content, contact list (Anglano, 2014; Mahajan et al., 2013). DB Browser for SQLite graphical user interface is shown in Fig. 3.

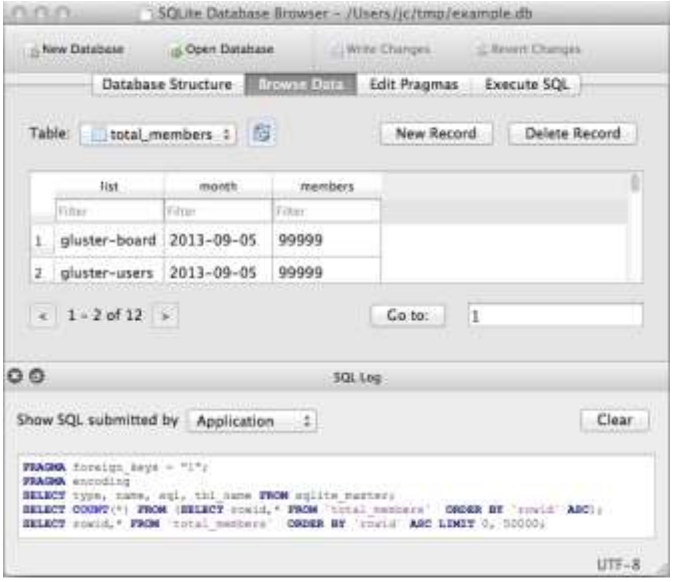
[4] http://www.technoduce.com

[5] http://postini-solutions.com

[6] https://www.secway.fr

[7] http://sqlitebrowser.org

[8] http://www.sqlite.org



	list	month	members
1	gluster-board	2013-09-05	99999
2	gluster-users	2013-09-05	99999

```
PRAGMA foreign_keys = "1";
PRAGMA encoding
SELECT type, name, sql, tbl_name FROM sqlite_master;
SELECT COUNT(*) FROM (SELECT rowid,* FROM `total_members`  ORDER BY `rowid` ASC);
SELECT rowid,* FROM `total_members`  ORDER BY `rowid` ASC LIMIT 0, 50000;
```

Fig. 3. *DB Browser for SQLite graphical user interface ("DB Browser for SQLite," n.d).*

2.3. Wireshark

Wireshark[9] is a multi-platform, open-source network protocol analyzer that captures, analyzes, and filters network traffic (Kendall, 2007). Wireshark provides a graphical user interface to start-stop packet capturing and analyze captured packets as it is shown in Fig. 4. Barghuthi and Said (Barghuthi and Said, 2013) used Wireshark to analyze instant message encryptions of several instant messengers.

3. Instant Messaging Encryption Tools & Methods

In this section, commonly used instant messaging encryption tools and methods such as secure socket layers, off-the-record messaging and private browsing are described.

3.1. Secure Sockets Layer (SSL)

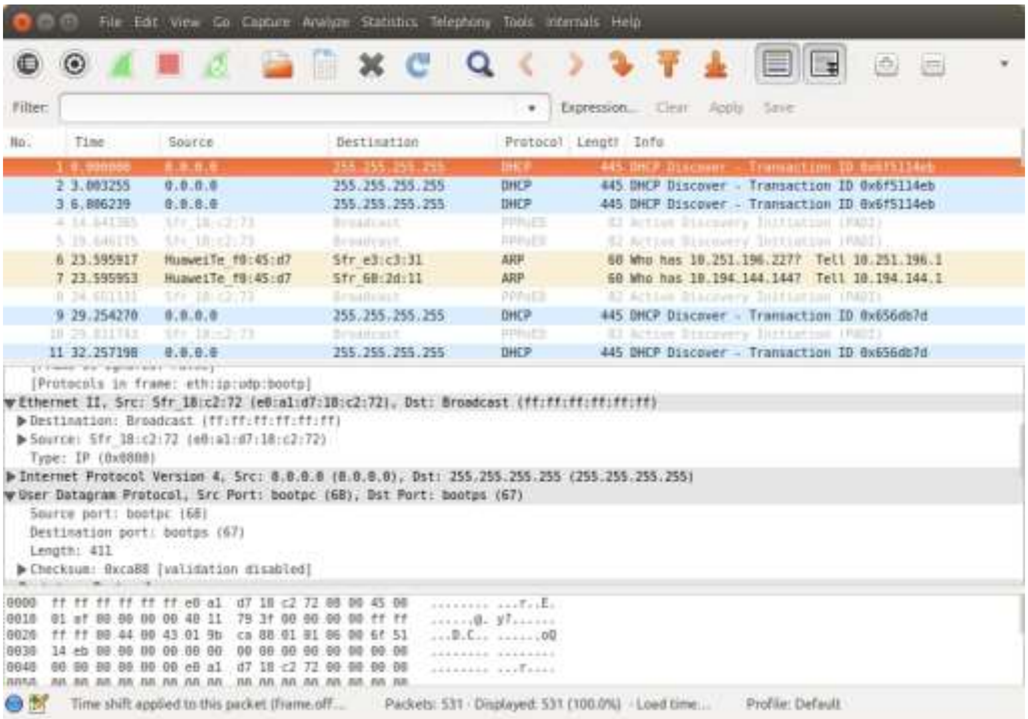
Secure Sockets Layer (SSL) is the most widely deployed and used security protocol on the internet that offers encryption, source authentication and integrity protection for data exchanged over insecure, public networks (Gupta et al., 2002). SSL has the flexibility to accommodate different cryptographic algorithms for key agreement, encryption and hashing (Gupta et al., 2002). SSL has two main components:

- Handshake protocol provides negotiation between SSL client and server in order to authenticate each other and establish a shared master secret using public-key cryptographic algorithms (Gupta et al., 2002).
- Record layer formats application protocol messages with providing a header for each message and a hash that is generated from Message Authentication Code (MAC) (McKinley, 2003).

SSL handshake process is shown in Fig. 5 and its steps can be listed as ("The good-to-know's of SSL and SSL Certificates," 2009):

- Browser requests a secure session from web server.
- Web server responses this request by sending its certificate that contains information about the site and the established connection such as certificate authority, connection protocol version, and key exchange mechanism.
- If the browser verifies the certificate, it sends a one-time session key that is encrypted with server's public key.
- Server decrypts this one-time session key using its private key.

[9] https://www.wireshark.org


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source             Destination       Protocol Length Info
   1 0.000000    0.0.0.0            255.255.255.255   DHCP     445 DHCP Discover - Transaction ID 0x6f5114eb
   2 3.003255    0.0.0.0            255.255.255.255   DHCP     445 DHCP Discover - Transaction ID 0x6f5114eb
   3 6.006239    0.0.0.0            255.255.255.255   DHCP     445 DHCP Discover - Transaction ID 0x6f5114eb
   4 14.641385   Sfr_18:c2:73       Broadcast         PPPoED    82 Active Discovery Initiation (PADI)
   5 19.646175   Sfr_18:c2:73       Broadcast         PPPoED    82 Active Discovery Initiation (PADI)
   6 23.595917   HuaweiTe_f0:45:d7  Sfr_e3:c3:31      ARP       60 Who has 10.251.196.227?  Tell 10.251.196.1
   7 23.595953   HuaweiTe_f0:45:d7  Sfr_68:2d:11      ARP       60 Who has 10.194.144.144?  Tell 10.194.144.1
   8 24.651111   Sfr_18:c2:73       Broadcast         PPPoED    82 Active Discovery Initiation (PADI)
   9 29.254270   0.0.0.0            255.255.255.255   DHCP     445 DHCP Discover - Transaction ID 0x656db7d
  10 29.811743   Sfr_18:c2:73       Broadcast         PPPoED    83 Active Discovery Initiation (PADI)
  11 32.257198   0.0.0.0            255.255.255.255   DHCP     445 DHCP Discover - Transaction ID 0x656db7d

    [Protocols in frame: eth:ip:udp:bootp]
▼Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶Source: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
    Type: IP (0x0800)
▶Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▼User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 411
  ▶Checksum: 0xca88 [validation disabled]

0000  ff ff ff ff ff ff e0 a1  d7 18 c2 72 08 00 45 00   ........ ...r..E.
0010  01 af 00 00 00 00 40 11  79 3f 00 00 00 00 ff ff   ......@. y?......
0020  ff ff 00 44 00 43 01 9b  ca 88 01 01 06 00 6f 51   ...D.C.. ......oQ
0030  14 eb 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 e0 a1  d7 18 c2 72 00 00 00 00   ........ ...r....

Time shift applied to this packet (frame.off...   Packets: 531 · Displayed: 531 (100.0%) · Load time...   Profile: Default
```

Fig. 4. Wireshark graphical user interface

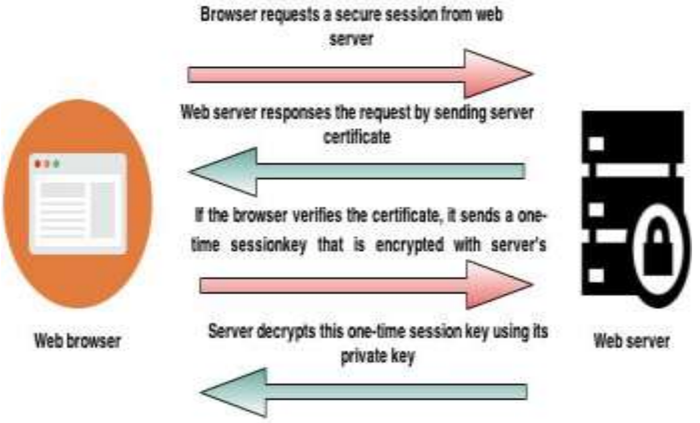

Browser requests a secure session from web server
Web server responses the request by sending server certificate
If the browser verifies the certificate, it sends a one-time sessionkey that is encrypted with server's
Server decrypts this one-time session key using its private key
Web browser
Web server

Fig. 5. *SSL handshake process*

3.2. Off-the-Record (OTR) Messaging

Off-the-record (OTR) messaging is a software that provides private conversations over instant messaging with providing encryption, authentication, perfect forward secrecy, deniability and integrity (Bonneau and Morrison, n.d.; Goldberg, 2006). OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie–Hellman key exchange with 1536 bits group size, and the SHA-1 hash function ("Off-the-Record Messsaging," 2014).

3.3. Private Browsing

Private browsing keeps the entire browsing session private by not recording your history of pages visited, by blocking all cookies and temporary internet files that visited websites use (Harvell, 2013; Schneider et al., 2009; Schneider and Evans, 2012). In addition to this, private browsing blocks all installed third-party extensions by default. All modern web browsers such as Google Chrome, Mozilla Firefox, Apple Safari, Opera, and Microsoft Internet Explorer support private browsing. Authors recommend to use web-based instant messaging applications in private browsing mode.

4. Results and Discussion

Instant messengers' encryption methods differ through installed devices. Barghuthi and Said (Barghuthi and Said, 2013) compares instant messaging encrypting methods for three different platforms: (1) Personal computers (PC), (2) web clients, (3) mobile devices. Instant messengers' encryption methods are compared through text conversations. Table 1 presents instant messengers' encryption methods comparisons for PC and Table 2 presents instant messengers' encryption methods comparisons for mobile.

Table 1. *Comparison of instant messengers' encryptions for PC (Barghuthi and Said, 2013)*

Messenger	**Text conversation sent over internet**	**Text conversation after encryption**	**Text conversation after enabling SSL**
Skype	Encrypted message	Encrypted message	-
Facebook Web Messenger	Plain text	-	Encrypted message
Gmail Web Messenger	Encrypted message	-	Encrypted message
Yahoo Web Messenger	Encrypted message	Encrypted message	-

Messenger	Text conversation sent over internet	Text conversation after encryption	Text conversation after enabling SSL
eBuddy Web Messenger	Plain text	-	Plain text
Google Talk Web Messenger	Plain text	-	Encrypted message

Table 2. Comparison of instant messengers' encryptions for mobile (Barghuthi and Said, 2013)

Messenger	Text conversation sent over internet	Text conversation after encryption	Text conversation after enabling SSL
Skype	Encrypted message	-	-
Facebook Web Messenger	Plain text	-	-
Gmail Web Messenger	Plain text	-	-
Yahoo Web Messenger	Encrypted message	Encrypted message	Encrypted message
eBuddy Web Messenger	Plain text	-	Encrypted message
Google Talk Web Messenger	Plain text	-	Encrypted message

5. Conclusion

Security requirements for instant messengers depend the platform they target. For example, a web-based instant messenger does not in need to store artifacts. But it is a critical process for both PC and mobile instant messengers. These requirements can be combined into a list such as:

- Messages should be sent through SSL protocol
- Web-based instant messengers should service over HTTPS
- If the browser does not support SSL protocol, Virtual Private Network (VPN) should be used to connect a SSL proxy server
- Web-based instant messengers should be used in private browsing mode
- If instant messenger does not encrypt messages, an encryption tool such as Simp must be used for security

References

Anglano, C., 2014. Forensic analysis of WhatsApp Messenger on Android smartphones. Digit. Investig. 11, 201–213. doi:10.1016/j.diin.2014.04.003.

Barghuthi, N.B. Al, Said, H., 2013. Social Networks IM Forensics: Encryption Analysis. J. Commun. 8.

Bodriagov, O., Buchegger, S., 2011. Encryption for peer-to-peer social networks, in: Proceedings - 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing, PASSAT/SocialCom 2011. pp. 1302–1309. doi:10.1109/PASSAT/SocialCom.2011.158.

Bonneau, J., Morrison, A., n.d. Finite-State Security Analysis of OTR Version 2. Analysis 2–6.

DB Browser for SQLite [WWW Document], n.d. URL http://sqlitebrowser.org (accessed 27.01.15).

Global Information Security Survey: 2015 Results by Industry [WWW Document], 2015. PricewaterhouseCoopers. URL http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml (accessed 27.01.15).

Goldberg, I., 2006. Off-the-Record Messaging.

Gupta, V., Gupta, S., Chang, S., Stebila, D., 2002. Performance analysis of elliptic curve cryptography for SSL, in: WiSE ’02: Proceedings of the 1st ACM Workshop on Wireless Security. pp. 87–94. doi:10.1145/570681.570691.

Harvell, B., 2013. iConnected: Use AirPlay, iCloud, Apps, and More to Bring Your Apple Devices Together, 1st ed. Wiley.

Infographic Top 10 Most Popular Instant Messaging Apps In The World [WWW Document], 2014. URL http://www.infographicscreator.com/2014/08/30/infographic-top-10-most-popular-instant-messaging-apps-in-the-world/ (accessed 27.01.15).

Instant messaging targeted for malicious worm attack [WWW Document], 2006. . ComputerWeekly. URL http://www.computerweekly.com/feature/Instant-messaging-targeted-for-malicious-worm-attack (accessed 27.01.15).

Kendall, K., 2007. Practical Malware Analysis, Black Hat Conference, USA. doi:10.1016/S1353-4858(12)70109-5.

Mahajan, A., Dahiya, M., Sanghvi, H., 2013. Forensic Analysis of Instant Messenger Applications on Android Devices. Int. J. Comput. Appl. 68, 38–44. doi:10.5120/11602-6965.

McKinley, H.L., 2003. SSL and TLS: A Beginners Guide, Information Security.

Off-the-Record Messsaging [WWW Document], 2014. . Wikipedia. URL http://en.wikipedia.org/wiki/Off-the-Record_Messaging (accessed 27.01.15).

Owens, M., 2003. Embedding an SQL database with SQLite. Linux J. 2003, 2.

Sanchez, J., 2014. Malicious Threats, Vulnerabilities and Defenses in WhatsApp and Mobile Instant Messaging Platforms.

Schneider, G., Evans, J., Pinard, K.T., 2009. The Internet - Illustrated, 6th ed. Cengage Learning.

Schneider, G.P., Evans, J., 2012. New Perspectives on the Internet: Comprehensive, 9th ed. Cengage Learning.

Secway [WWW Document], n.d. URL https://www.secway.fr (accessed 27.01.15).

The good-to-know's of SSL and SSL Certificates [WWW Document], 2009. doteasy. URL http://blog.doteasy.com/2009/06/15/the-good-to-knows-of-ssl-and-ssl-certificates/ (accessed 27.01.15).

Yusof, M.K., Abidin, A.F.A., 2011. A secure private instant messenger, in: 17th Asia-Pacific Conference on Communications, APCC 2011. pp. 821–825. doi:10.1109/APCC.2011.6152921.