A Secure Messaging and File Transfer Application

Sandhya Armoogum
Dept. Industrial Systems & Engineering
University of Technology, Mauritius (UTM)
La Tour Koenig, Mauritius
asandya@umail.utm.ac.mu

Sanjeet Kumar Mudhoo
Dept. Industrial Systems & Engineering
University of Technology, Mauritius (UTM)
La Tour Koenig, Mauritius
ravi.mudhoo@hotmail.com

***Abstract*— Instant Messaging (IM) is becoming more and more popular and ubiquitous as it is accessible via mobile devices. However, many existing IM applications do not provide much security. This is a serious limitations of IM systems especially when IM is being used in the workplace as a communications tool. In this paper, we present the different security vulnerabilities associated with communication using IM, as well as the security provided in some IM applications. Finally, we describe the design and implementation of a simple secure lightweight application for secure messaging and file transfer.**

Keywords- Privacy; Instant Messaging; Encryption; Security; Secure Communication.

I. INTRODUCTION

Instant Messaging (IM) is a type of communication service over the Internet that enables individuals to exchange text messages, share files (images, videos and documents) and track availability of a list of users in real-time. IM is popularly used for communications at large. Almost everybody nowadays is familiar with such messaging system as Skype, Instagram, Google Hangouts, Facebook Messenger, WhatsApp and Viber. However, IM services over the last few years have evolved from a casual communication tool to an indispensable and unified communication tool in the workplace, designed to enable rapid response text-based conversation, encourage enterprise collaboration through file sharing and even video conferencing. In a survey conducted in February 2016 by BetterCloud involving 801 respondents[1], it is reported that just 13% of respondents are not using real-time instant messaging for work purposes; 56% of respondents believe that real-time messaging will displace email as their organization's primary workplace communication and collaboration tool; 83% of respondents agree that IM improves communication in the workplace; and more employees report an increase in productivity rather than decrease (only 24% of respondents believe that IM is a distraction and decreases productivity). Currently, IM is not only being used by Startups but also by small and medium organizations, as well as large enterprises. In a survey conducted by SoftwareAdvice [18], 75% of employees using IM reported decreased call and email volume, while 66% of employees reported that the quick resolution of simple questions helped increase productivity.

Similarly, in [2][3], the authors support that IM is an effective communication tool that can enhance the quality of work-related communication and relationship, and thus enhance the organisational agility. Indeed, IM provides an efficient way of communicating and resolving issues quickly, increasing collaboration on projects and reducing the need for meetings, reducing interruption, improving customer service, which help enhance productivity, as well as fostering good relationships. IM can be particularly helpful in communication between geographically separated co-worker or students engaged in distance learning.

As IM gains popularity, particularly for businesses it has also increasingly become the target of attacks [4]. The need for security in such systems becomes important. One such security requirement is confidentiality/privacy, which is becoming very challenging in the face of widespread Internet surveillance. Using simple and free sniffing software, anyone can easily capture data being transmitted in a network.

According to the Electronic Frontier Foundation (EFF), there has been ample evidence that authoritarian governments around the world are relying on technology to facilitate human rights abuses such as listening to voice calls, read emails and text messages [5]. In [6], the author claims that our privacy is slowing eroding and that in the future it would be very difficult to remain anonymous and not have a digital trail. With the advent of "Big Data", sophisticated and inexpensive data mining tools reveal increasing amounts of personal information. Nevertheless, it is believed that making surveillance expensive by employing good security techniques, such as strong encryption is the best defence.

In this paper, we present a secure messaging and file transfer application, which allows a user to communicate securely with another user or group of users. The paper is organized as follows. Existing IM applications and their security are described in Section 2. Section 3, presents the proposed secure messaging and file transfer application. In Section 4, the proposed system is evaluated. Finally, we draw conclusions in the Section 5.

II. EXISTING MESSAGING SYSTEM & SECURITY

When using IM, the user feels like he/she is directly connected to the recipient, but most IM systems are designed and deployed with a client-server architecture. The user installs a client software of the IM application and creates an account. Most IM systems implement some form of authentication to identify the user and hence does not provide anonymous communication. When a user sends a message to another user, the IM client encapsulates the

 ISBN: 978-1-61208-513-5

message into a packet and send it to the IM server, which looks at the recipient and send the packet to the destination if the receiver is online [7]. If the recipient is not online, the undelivered message is held in the server until it can be delivered. Fig. 1 below shows the client-server IM infrastructure and communication process.

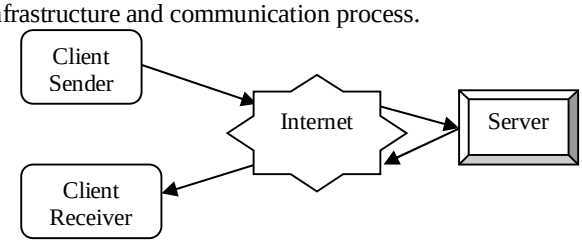

Figure 1. Instant Messaging Infrastructure and Communication Process.

The IM system has several security vulnerabilities. Considering the Microsoft STRIDE Threat Modeling Methodology, IM systems are particularly vulnerable to **S**poofing, **T**ampering of messages, **R**epudiation attacks, **I**nformation disclosure due to eavesdropping and **D**enial of Service attacks. Security mechanisms are required to secure IM systems. Typically, if messages are sent in clear text, the messages can be read; message contents, sender or receiver information can be modified while the message is in transit or while it is stored on the server. Similarly, the IM server can be victim to Denial of Service attack (DoS) and be unavailable for a certain period of time. On the 31st December 2015, WhatsApp was reported to be down temporarily due to the heavy traffic load (which mimics a Distributed Denial of Service (DDoS)) it experienced [8].

In November 2014, the EEF started the Secure Messaging Scorecard where they evaluate the security of the popular messaging system used [9]. The criteria that were used to assess the security of the messaging system were as follows: (i) encryption of data along transmission links with a key not accessible to the provider, (ii) ability to verify the correspondent's identity, (iii) forward secrecy, (iv) whether the code is open to independent review, (v) whether the crypto design is well documented, and (vi) if the messaging tool has been open to independent security audit. Figs. 2-7 depict the resulting scorecard of the following popular messaging tool: Google Hangouts, Facebook chat, Skype, Viber, WhatsApp, and Yahoo Messenger [9].

Figure 2. Hangouts Scorecard [9].

Figure 3. Facebook Chat [9].

Figure 4. Skype Scorecard [9].

Figure 5. Viber Scorecard [9].

Figure 6. WhatsApp Scorecard [9].

Figure 7. Yahoo! Messenger Scorecard [9].

As can be seen from the Scorecards of popular messaging system above, most of the messaging tool do not provide much security except for WhatsApp, which very recently released an update to include encryption of messages for security [10]. WhatsApp now provides end-to-end encryption of messages, calls, videos, images and files.

Skype, a popular communication tool at the workplace, is a telecommunications application software product that provides messaging, video chat and voice calls for computers, tablets, and mobile devices. Skype runs on most of the popular platforms today. Users can send instant messages, exchange files and images, send video messages, and create conference calls with Skype. Skype was purchased by Microsoft corporation in 2011. In 2013, a report by Ars Technica claims that Microsoft can regularly scan message content for signs of fraud, and company managers may log the results indefinitely and this can only happen if Microsoft can access and convert the messages into human-readable form [11].

Documents leaked by Edward Snowden (the whistleblower), showed that the Government Communications Headquarters (GCHQ), which is a British intelligence and security organization, has access to emails and messages that the National Security Agency (NSA) siphons off directly and en masse from Google, Skype and

 ISBN: 978-1-61208-513-5

Facebook; the NSA collects 194m text messages and 5bn location records every day [12]. Just recently, in February 2015, the UK surveillance tribunal ruled that GCHQ acted unlawfully in accessing millions of private communications collected by the NSA up until December 2014 [13].

Facebook employs a technology that scans posts and chats for criminal activity, which clearly means that messages users send are subject to surveillance and is a violation of privacy [14]. This monitoring came to light in 2012, when a man is his thirties was chatting with a 13-year old female minor from South Florida. With Facebook's help, the police were able to arrest the suspected pedophile [15]. It is thus clear that messaging systems need to provide security to achieve confidentiality of communications.

Moreover, anonymity is also another important security requirement of messaging systems. It is usually preferred that someone sniffing data packets on the Internet is not only unable to read the message contents but is also not able to link the messages to the people sending or receiving them. Many users concerned with privacy, such as activists, oppressed people, journalists and whistleblowers, as well as the average person, often make use of an anonymous overlay networks such as the Invisible Internet Project (I2P) and The Onion Routing Network (TOR) for secure communication. Both the I2P and TOR provides anonymous, confidential exchange of messages by the means of cryptography. However, a recent publication by the University of Cambridge, the University of California-Berkeley, and the University College London in February 2016 confirms that users of such anonymous overlay networks are commonly blocked from accessing websites and anonymous users are being treated as second-class Web citizens [16]. Likewise, many organisations attempt to block TOR data packets and the use of the TOR browser, which is commonly used to access the DarkNet, by means of port filtering inside their network to protect themselves from malware, DarkNet access by their employees and other attacks. Still, most commonly used IM systems do not provide anonymous communication feature.

Several secure messaging systems have been proposed and developed in both academia and industry. In [17], the authors present a Systemization Methodology, which divide the security requirements of a secure messaging system into three nearly orthogonal problem areas namely (1) trust establishment, (2) conversation security and (3) transport privacy. The trust establishment relates to the authentication of the communicating parties as well as the distribution of cryptographic keys, whereas conversation security ensures the protection of the exchanged messages & files during conversations. Finally, transport privacy implies the hiding of the communication metadata. In [19], a messaging system called Riposte that allows a large number of clients to anonymously post messages to a shared "bulletin board," is proposed. Riposte mainly provides protection against traffic analysis. In [20], a secure IM system is proposed, which uses identity-based cryptosystems to provide strong authentication and secure communication (confidentiality, integrity and non-repudiation).

Our proposed system, takes a practical approach and adopts well established security mechanisms to provide a simple, lightweight messaging system which provides (i) confidentiality and privacy of messages & files transferred; (ii) a secure channel of communication between two users; (iii) anonymous communication; and (iv) scalability whereby a group of users can chat and share files. In the next Section, we describe the design and implementation of the proposed messaging system.

III. Design and Implementation of the Secure Messaging and File Transfer Application

Most commercial IM infrastructure allows the transfer of messages via a messaging server as shown in Fig 1 [20]. However, the presence of a third-party server where messages may be temporarily or permanently stored poses several privacy issues. A breach of the IM server may allow attackers to access all messages and files shared. In our proposed system, we do not involve a messaging server, whereby the users chat and exchange files with one another directly as depicted by Fig 8. The disadvantage of adopting this approach however is that communication is only possible when the two communicating parties are online. However, the security benefits are tremendous, as messages and files are not being stored in an intermediate node, and are thus not vulnerable to unauthorized access. Messages exchanged can be cached on the recipient's computer if required by the implementation of a log file. Files, which can be transferred include text documents, PDFs, pictures, audio and video amongst others, is also stored on the recipient's computer. Our proposed system also provides a secure channel for communication between two or more users. A virtual private network (VPN) is a well-established technology that creates a secure and often encrypted connection over a less secure network. A remote-access VPN uses a public telecommunication infrastructure like the internet to provide remote users with a secure channel for communication to another user or network. This is especially important when employees and users are using a public Wi-Fi hotspot or other avenues to use the internet to connect to one another user ubiquitously.

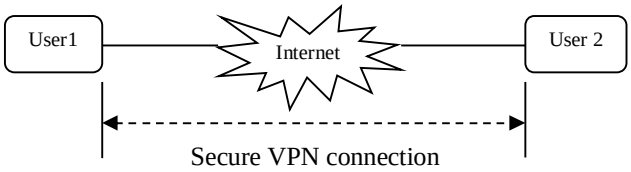

Figure 8. Proposed System layout .

Two users wishing to engage in a secure chat and file transfer, first have to establish a secure VPN network connection. The LogMeIn Hamachi [21], hosted VPN service software, is used to set up the VPN, which allows to set up secure connections between the two users. First LogMeIn Hamachi is installed. When this client software runs, it implements a virtual network adapter, and the computer is assigned an additional IP address that identifies

the computer on any virtual network that is joined. The user can then create a virtual network by name and assign it a password; or join an existing virtual network. All users who wishes to communicate can be asked to join the network created. The users have to install the VPN client software and select the network by connecting to it by name, and supplying the password. Similarly, different networks can be created for different groups of communicating friends, collaborating employees etc. The use of a VPN solution to establish the network connections ensures a secure channel for communication, thereby providing both conversation security as well as transport privacy. At all point, the VPN software allows to view which users (users' nicknames displayed) are connected and are online at a particular point in time. This approach to establish a secure connection supports anonymous communication given that the users are not required to identify themselves by means of their email address or telephone numbers. The assigned IP address of the VPN client is thus not linked to a user identifier. Moreover, this approach also supports some level of trust regarding the person(s) with whom the chat or the file transfer is taking place, as the user could only join the network and participate only if the user has been provided with the network name and password. The proposed system implementation provides a user interface, which allows the application user to perform different functionalities such as choosing which user(s) to securely communicate with. Fig. 9 shows the Use Case diagram of the application user.

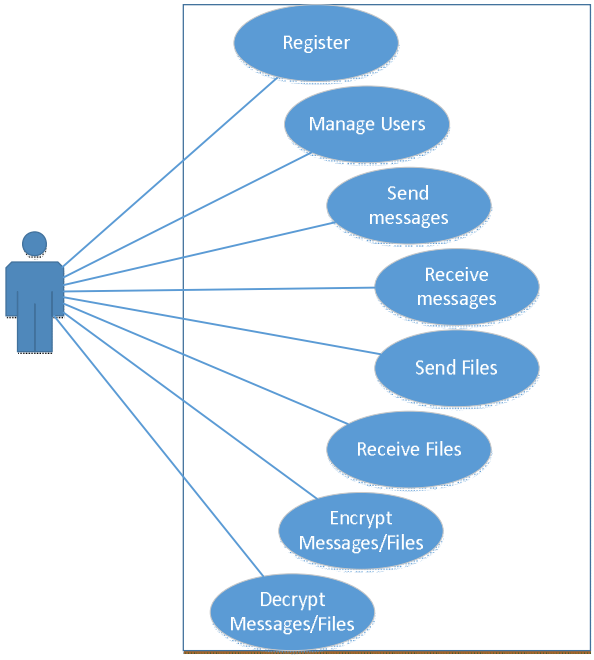

Figure 9. Use Case diagram of a Chat Application User.

Though the VPN connection ensures that messages or files are transferred securely i.e., in encrypted form, the application does not rely on the VPN connection for security but rather implements its own security mechanism for providing confidentiality and privacy of messages and files transferred, as a VPN can be attacked in various ways [22]. Two different approaches are used for providing confidentiality in the proposed system: (1) encryption of messages using public key cryptography, and (2) encryption of files to be transferred using symmetric cryptography.

For every chat instance with a particular user, the application on each users' computer generates a pair of public key cryptography key. The public key is shared with the user with whom communication is intended, while the private key is cached on the users' respective computer. When a user type a message, the message is encrypted using the public key of the recipient and sent to the recipient. The recipient uses his/her private key to decrypt the message as shown in Fig. 10. The use of Public Key Cryptography for encryption and decryption of messages is acceptable despite the fact that Public key encryption is much slower than symmetric cryptography, because the length of each message is usually limited in IM systems. Short Message Service (SMS) messages are limited to 160 characters, while Twitter messages are limited to 140 characters. In the application, the message length was limited to 140 characters.

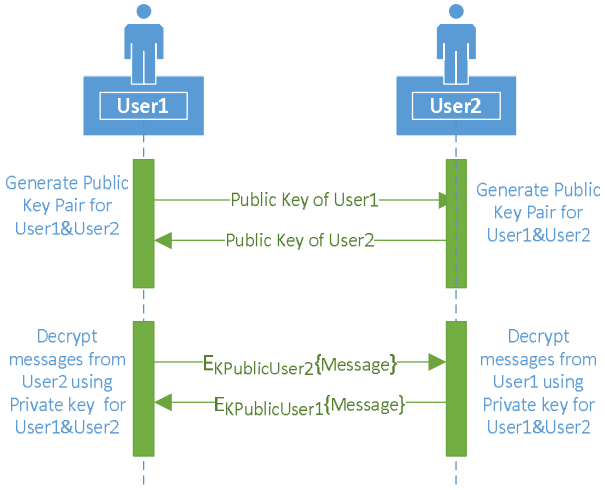

Figure 10. Encryption and Decryption of messages for secure chat.

For securing the files to be transferred between two users, Public Key Cryptography being slow, Symmetric Cryptography is chosen for efficiency, especially considering that the files can be of significant size. Prior to starting a file transfer, the application requests the sender to select a password for locking the file. This password is sent as an encrypted message to the receiver and is thus not at risk of interception. This securely shared password is the basis for deriving the symmetric key, which is to be used for the encryption of the file by the sender, as well as the decryption of the received encrypted file by the receiver. To generate a symmetric key, it is proposed to use a cryptographic hash function to process the password producing a fixed length output (hash code), which can be used as the key. The hash code, i.e., key derived, is strongly dependent on the

 ISBN: 978-1-61208-513-5

password; any change in the password results in a different hash code. Fig. 11 depicts the secure processing of files transferred. Files received are automatically decrypted and stored in a download folder associated with the application. For enhanced security, the application is designed to validate the password and ensure that a strong password is selected by the sender for locking the file. A weak password may be easily guessed by an attacker, who may then use the password to derive the encryption key and thus successfully decrypt files being transferred.

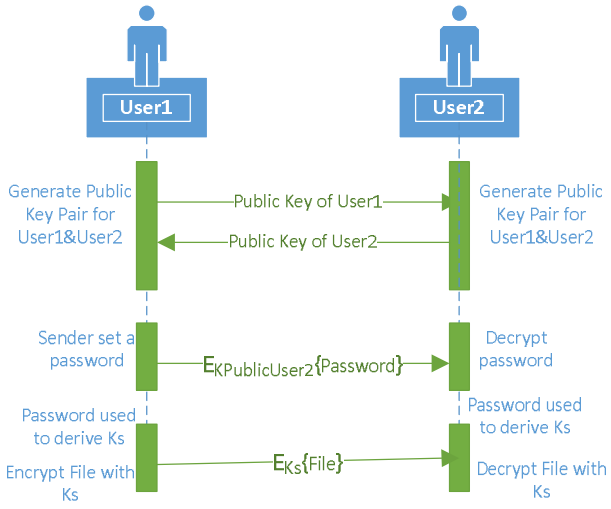

Figure 11. Encryption and Decryption of Files to be transferred securely.

The secure messaging and file transfer application was implemented using Visual Studio. The RSA public key encryption was used for encryption and decryption of the messages. The RSACryptoServiceProvider in .NET was used. When using the default constructor as shown below to create a new instance of the RSA algorithm, a pair of public and private key pair are created by default.

```
RSACryptoServiceProvider rsa = new
        RSACryptoServiceProvider(512);
```

The key pair generated was extracted using the ToXMLString method, which returns an XML representation of the key, which is saved to disk as an XML file. The private key and the public key are captured as follows respectively.

```
rsa.ToXmlString(true)
rsa.ToXmlString(false)
```

The private key is never shared but stored on the key owner's computer, which implies that it safe unless the user's computer is breached. The proposed system can easily be installed and used by any user anywhere, as it does not require users to have digital certificates etc. Fresh keys can be generated for each new chat sessions for each user. This simple, lightweight application is also easily scalable, allowing any number of users to use it to communicate securely and to transfer files.

For the encryption of files, using symmetric encryption, the Rijndael (Advanced Encryption Standard - AES) algorithm was chosen. Instead of using the usual cryptographic hash algorithm for deriving the symmetric key to be used for encrypting files, the Rfc2898DeriveBytes class is used. This class implements a password-based key derivation functionality, PBKDF2, by using a pseudo-random number generator based on the cryptographic hash function HMACSHA1. Moreover, the IM application also has a feature, which allows the user to create chat logs for chat sessions to keep a history of messages exchanged. However, if users prefer not to keep a copy of messages exchanged i.e., if they are using a computer from a library, this feature can be disabled so as to leave no trace of the conversation on that machine.

IV. EVALUATION

The secure chat application is evaluated on the following three criteria: (1) Security and Privacy Properties, (2) Usability Properties, and (3) Ease of Adoption.

The use of the VPN software allows to set a secure underlying network to carry the messages and/or files to be transferred. However, given that the user has no control over the encryption of the messages for transmission over the VPN tunnel, the application does not depend on the VPN network for security. The VPN connection is rather an added benefit, as it provides a means for users to choose who they want to invite in the network for communication. For confidentiality of messages exchanged, the system makes use of the RSA public key cryptography algorithm for encryption. This ensures that the messages sent are private and can only be read by the communicating parties. Attackers sniffing on the network will only capture the encrypted messages, which have been further encrypted by the VPN software. Similarly, the well established and secure AES algorithm is used for the encryption of files to be transferred for confidentiality.

The user interface of the system is simple and intuitive and offers the basic functionality of chat and file transfer. The key generation and sharing is transparently conducted by the system when the user chooses the recipient to whom he/she wants to send a message. The deployment of the proposed system is also simple; it involves the installation and network setup of the VPN, followed by the installation of the secure messaging and file transfer application.

Such a simple and lightweight application can be used for secure messaging by journalists, for collaboration between employees in business organisations, by distance learning/e-learning students for communication and submission of their electronic assignments amongst others.

V. CONCLUSION

In this paper, a simple, practical, lightweight and secure messaging application was proposed, which is based on the use of a VPN connection and Cryptography for security. Such an application can be easily deployed and used for secure, anonymous communication between users. Given that this application is designed such that it is not a client server, store and forward system, the network connectivity among different users can be a challenge. An important implication of this design choice is that chat and file transfer

 ISBN: 978-1-61208-513-5

is only possible when the recipient is online. However, the absence of a caching server also enhances the security of the system. Furthermore, the proposed system does not rely on the VPN software for security of messages and files during the transfer but rather uses well established cryptographic algorithms for providing confidentiality within the application. The application can easily be used by people looking for anonymity and is easily scalable as keys are dynamically generated when required. Future work on the application involves addressing the out of band transmission of the network name and password for establishing secure and trusted connections with users. Another improvement on the application may be to allow users the choice to authenticate participants or communicate anonymously.

REFERENCES

[1] Scott Solomon, *Real-Time Messaging: Data Unearths Surprising Findings on Usage, Distraction, and Organizational Impact*" March 3, 2016 available at https://www.bettercloud.com/monitor/real-time-enterprise-messaging-comparison-data/ last accessed 20.09.2016

[2] C. X. J. Ou, R. N. Davison, Y. Liang and X. Zhong, *The Significance of Instant Messaging at Work*, Fifth International Conference on Internet and Web Applications and Services (ICIW), 2010, Barcelona, 2010, pp. 102-109

[3] Hanif Suhairi Abu Bakar, Nor Azmi Hj. Johari, *Instant Messaging: The Next Best Knowledge Sharing Tools in a Workplace After Email* in the Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT2009), Beijing, 2009, pp. 268-269.

[4] Neal Leavitt, *Instant Messaging: A New Target for Hackers*, Computer magazine, Published by the IEEE Computer Society, July 2005

[5] *Mass Surveillance Technologies*, available at https://www.eff.org/issues/mass-surveillance-technologies. Last accessed 12.08.2016

[6] Jeffrey MacKie-Mason, *Can We Afford Privacy from Surveillance*? University of Michigan, Copublished by the IEEE Computer and Reliability Societies Sep/Oct 2014.

[7] Craig Sweigart, *Instant Messaging Security*, Global Information Assurance Certification Paper, SANS Institute, 2003

[8] Victoria Woollaston, *WhatsApp apologises as service crashes on New Year's Eve*, available at http://www.dailymail.co.uk/sciencetech/article-3380408/WhatsApp-goes-Users-Europe-report-problems-connecting-chats-messaging-app.html#ixzz4EHfs6Xdg

[9] Electronic Frontiers Foundation, *Which apps and tools actually keep your messages safe?* Web Article, available at https://www.eff.org/node/82654

[10] Bill Budington, *WhatsApp Rolls Out End-To-End Encryption to its Over One Billion Users*, available at https://www.eff.org/deeplinks/2016/04/whatsapp-rolls-out-end-end-encryption-its-1bn-users, April 7, 2016 .

[11] Dan Goodin, *Think your Skype messages get end-to-end encryption? Think again*, May 20, 2013, available at http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/

[12] Carly Nyst, *Today is a great victory against GCHQ, the NSA and the surveillance state* available at https://www.theguardian.com/commentisfree/2015/feb/06/great-victory-against-gchq-nsa-surveillance-state, February 2015

[13] Eric King, *Victory! UK surveillance tribunal finds GCHQ-NSA intelligence sharing unlawful* February 2015, available at https://www.privacyinternational.org/node/485

[14] Joseph Menn, *Social networks scan for sexual predators, with uneven results*, Jul 12, 2012 available at http://www.reuters.com/article/us-usa-internet-predators-idUSBRE86B05G20120712

[15] Jared Howe, *Why Your Facebook Chats are Being Monitored*, January 2016, available at http://blog.privatewifi.com/your-facebook-chats-are-being-monitored-find-out-why-the-social-media-privacy-report/

[16] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch and Damon McCoy, *Do You See What I See? Differential Treatment of Anonymous Users*. In the proceedings of the Internet Society Network and Distributed System Security Symposium 2016 (NDSS'16), February 2016, San Diego, CA, USA

[17] Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, Matthew Smith, *SoK: Secure Messaging*, IEEE Symposium on Security and Privacy, 2015.

[18] Daniel Harris, *Boost Productivity With Online Chat Presence Displays*, SoftwareAdvice, available at http://www.softwareadvice.com/resources/boost-productivity-chat-presence/ last accessed 20.09.2016

[19] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières, *Riposte: An Anonymous Messaging System Handling Millions of Users*, in the 2015 IEEE Symposium on Security and Privacy, pp 321-338

[20] Raymond B. Jennings III, Erich M. Nahum, David P. Olshefski, Debanjan Saha, Zon-Yin Shae, and Chris Waters, *A Study of Internet Instant Messaging and Chat Protocols*, in IEEE Network, July/August 2006, pp 6-21

[21] LogMeIn Hamachi, *Create virtual private networks on-demand*, available at https://www.vpn.net/

[22] Spiegel Online, *NSA Documents Attacks on VPN, SSL, TLS, SSH, Tor*, avalaible at http://www.spiegel.de/international/world/nsa-documents-attacks-on-vpn-ssl-tls-ssh-tor-a-1010525.html.. Last accessed 21.09.2016.

 ISBN: 978-1-61208-513-5