Insert here your thesis' task.

Czech Technical University in Prague
Faculty of Information Technology
Department of Computer Systems

Master's thesis

TODO

Bc. Tomáš Sušánka

Supervisor: Ing. Josef Kokeš

10th February 2016

Acknowledgements

TODO

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended. In accordance with Article 46(6) of the Act, I hereby grant a nonexclusive authorization (license) to utilize this thesis, including any and all computer programs incorporated therein or attached thereto and all corresponding documentation (hereinafter collectively referred to as the "Work"), to any and all persons that wish to utilize the Work. Such persons are entitled to use the Work in any way (including for-profit purposes) that does not detract from its value. This authorization is not limited in terms of time, location and quantity. However, all persons that makes use of the above license shall be obliged to grant a license at least in the same scope as defined above with respect to each and every work that is created (wholly or in part) based on the Work, by modifying the Work, by combining the Work with another work, by including the Work in a collection of works or by adapting the Work (including translation), and at the same time make available the source code of such work at least in a way and scope that are comparable to the way and scope in which the source code of the Work is made available.

In Prague on 10th February 2016 .....

Czech Technical University in Prague
Faculty of Information Technology

Citation of this thesis

Sušánka, Tomáš. *TODO.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2016.

Abstrakt

TODO

Klíčová slova TODO

Abstract

TODO

Keywords TODO

Contents

List of Figures

List of Tables

Introduction

TODO

Chapter 1

Current security status of major IMs

This chapter contains thorough description of five selected Instant Messengers and its security related findings. Particular software versions are mostly an estimate based on a date some findings were published and the software changelog.

1.1 Selection

We selected the following five Instant Messenger applications. The selection was based on various criterions to create a diverse mixture of messengers. The criterions included user base, geographical origin, authors, proclaimed security, license, price and other. For ease of comparison we've decided to select messengers with support for mobile platforms. We've omitted Facebook Messenger, since it is owned by the very same company as WhatsApp, Facebook Inc [3].

1.1.1 WhatsApp[1]

Large user base and overall popularity of the application is one of the main reasons WhatsApp is included. With 1 billion active users it is the most used messenger at the moment.[2]

1.1.2 Telegram[2]

Telegram praises itself as safer than WhatsApp. It uses its own messaging protocol MTProto and argues for its security. Telegram's clients are open-

[1] https://www.whatsapp.com
[2] https://www.telegram.org

source but the server side is proprietary. The authors of Russian social network VK, Nikolaj Durov and Pavel Durov, are the creators of Telegram.

1.1.3 Signal[3]

TODO

1.1.4 Threema[4]

TODO

1.1.5 WeChat[5]

TODO

Table 1.1: Messengers

Name	**First release**	**License**	**User base**
WhatsApp	January 2010	Proprietary	990 million[6]
Telegram	August 2013	GPLv2/GPLv3/Proprietary	60 million[6]
Signal	July 2014	GPLv3	10 million[7]
Threema	December 2012	Proprietary	3.5 million [8]
WeChat	January 2011	Proprietary	600 million[9]

1.2 Security aspects

The Electronic Frontier Foundation maintains a scoreboard of messaging applications' security. It evaluates messengers based on these seven criteria [4]:

- **Are messages encrypted in transit?** All user communication is required to be encrypted. Encryption of metadata, such as phone numbers, usernames or dates, is not required.
- **Are messages encrypted so the provider can not access it?** All user messages need to be end-to-end encrypted, from the moment user sends a message to the moment the other party recieves it. No decrypting and re-encrypting may occur during that process. The private keys need to be generated at the endpoints, not on the centralized server. Any bulk

[3]https://www.whispersystems.org
[4]https://www.threema.ch
[5]https://www.wechat.com/en/
[6]As of September 2015.
[7]Signal's predecessor TextSecure as of December 2013.
[8]As of June 2015.
[9]As of August 2015.

data collection is therefore meaningless and no third-party may access the messages unless one party allows it.

- **Can user verify contacts' identity?** This requires a verification mechanism of the other side's identity to prevent Man-in-the-Middle attacks.
- **Are past communications secure if keys stolen?** All messages need to be encrypted with routinely changed keys. The forward secrecy minimizes consequences when a private key is stolen, becuase the key has only a short-time validity. This criterion requires end-to-end encryption, it is therefore directly dependent on the second criterion.
- **Is the code open to independent review?** Sufficient amount of source-code needs to be available to perform an independent code review. This protects from unintentional encryption flaws, back doors or bugs.
- **Is the cryptography design properly documented?** The cryptography behind the application needs to be described in detailed documentation.
- **Has there been any recent code audit?** An independent security review of the application is not older than 12 months. This does not require the audit to be publicly available.

At the end of each chapter dedicated to one messenger a small note about the received score will be made.

1.3 WhatsApp

WhatsApp is a mobile messaging application. Besides text it enables users to send pictures, videos, voice and locations. WhatsApp Messenger is available for iPhone, BlackBerry, Windows Phone, Android and Symbian[5].

In February 2016 WhatsApp has reached 1 billion active users monthly and was the most used messenger to that moment [2].

The large user base and overall popularity of the application is one of the main reasons WhatsApp is included in this comparison.

Following section describes WhatsApp's security-related incidents.

1.3.1 Security-related incidents

1.3.1.1 Flaws in registration process

WhatsApp's user identity is bound to user's phone number. In order to verify the relationship user has to enter his phone number during the first start-up. WhatsApp server then sends SMS with verification code to such number. User

submits the code from the received text message and WhatsApp creates his account.

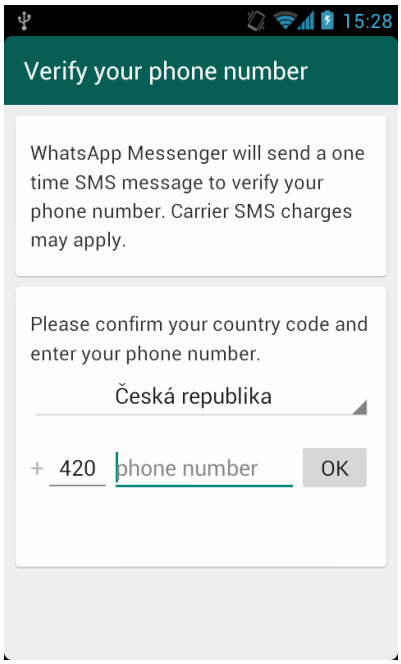


Figure 1.1: WhatsApp's registration process

Upto version 2.6.5 WhatsApp offered an alternative verification process. Instead of the user waiting for a text message, he was rather supposed to send a SMS to one of WhatsApp's phone numbers where he included his email. WhatsApp later sent verification code to the email and user verified himself with this code [6].

Serious drawbacks were found in this method in 2011 [7]. To hijack user's account attacker first opted for this method. Then using SMS spoofing service he sent SMS to WhatsApp's phone number pretending it originates from the victim. Attacker set the content of the message to an email he owned, leading to WhatsApp sending the verification code to the attacker. The attacker then simply entered the code from an email and successfully hijacked the victim's account.

Following these findings another method to bypass the registration process was published. During the registration phase WhatsApp sent a request for the verification SMS to be sent to the client in HTTP request similiar to this [6]:

Listing 1.1: HTTP request to dispatch SMS

```
GET [..]?to=4915143[..]&auth=659&[..] HTTP/1.1
User-Agent: WhatsApp/2.6.4 iPhone_OS/4.3.3 Device/iPhone_4
```

The request contained the final verification code in the GET parameter. That leads to a conclusion the client created the verification code, not the server, and expected user's confirmation. An attacker could simply intercept the request, retrieved the verification code and made sure the request didn't arrive to WhatsApp's servers to let the victim unaware of malicous intentions.

Attacker then created a fake HTTP OK response to let the messenger think the request was successful and entered retrieved verification code from the intercepted request. The attacker successfully hijacked the victim's WhatsApp identity and can both send and recieve all his messages.

The author of the research notified WhatsApp developers beforehand and WhatsApp fixed this issue before the research was made public [6]. To the date of writing this thesis WhatsApp doesn't offer discussed verification method anymore.

1.3.1.2 Password generation

WhatsApp uses lightly modified version of XMPP [8]. During the registration process it creates a username based on the user's phone number. In newer versions than 2.10 the password is generated on server's side [9]. However, older versions used the phone's IMEI number as password [9][10].

Listing 1.2: Pseudo-code of password generation on Android

```
md5(revert('IMEI'))
```

Any phone number – IMEI pair was therefore all an attacker needed to send messages on victim's behalf. Numerous applications are collecting plenty of user data and the IMEI and phone number might be among them. Any database leak with such information would lead directly to large accounts abuse.

1.3.1.3 Messages encryption

Up to version approximately 2.8 WhatsApp did not use any message encryption. The messenger used port 443 (commonly used for HTTPS) to send content, however it did not encrypt anything [11]. Using a simple network sniffer like Wireshark attacker was able to read all user's messages.

On May 2012 an application called "WhatsAppSniffer" had been released [12][1]. It abused described flaw and enabled attacker to see victim's messages in easy and lucid user interface.

On August 2012 WhatsApp started to use some sort of encryption. The developers did not reveal which protocol they use or any other information. Reports showed that simple message sniffing, as described in previous chapter, seized to work [13]. Some sources claim the RC4 stream cipher was used for encryption [14][15].

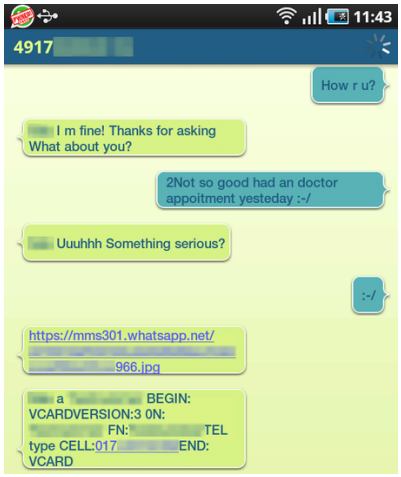


Figure 1.2: WhatsAppSniffer [1]

On November 18, 2014, Open Whisper Systems, the creators behind Signal messenger, announced a partnership with WhatsApp. The partnership should have escalated into incorporating OWS' encryption protocol to WhatsApp bringing end-to-end encryption to all WhatsApp clients. Open Whisper Systems stated: *"we are moving quickly towards a world where all WhatsApp users will get end-to-end encryption by default."*. [16]

WhatsApp confirmed this partnership, however did not comment it any further nor offered any further information. No additional information from Open Whisper Systems' side had been released as well. WhatsApp's FAQ currently only briefly states *"WhatsApp communication between your phone and our server is encrypted."*[17].

On April 2015, *heise.de* investigated the current state of WhatsApp's encryption. The journalists were sniffing messages using the Man-in-the-Middle technique. They showed that Android versions used end-to-end encryption and that the messages "*were encrypted according to the TextSecure protocol*"[18]. However, during testing the iOS client they concluded the messages weren't protected in such manner. Finally, they concluded they are unsure whether end-to-end encryption was actually used in all cases.

1.3.2 EFF's secure messaging score

At the time of writing, WhatsApp has two points out of seven in the EFF's secure messaging scorecard [4].

Table 1.2: WhatsApp's secure messaging score

Are messages encrypted in transit?	✓
Are messages encrypted so the provider can not access it?	✗
Can user verify contacts' identities?	✗
Are past communications secure if keys stolen?	✗
Is the code open to independent review?	✗
Is the cryptography design properly documented?	✗
Has there been any recent code audit?	✓

1.4 Telegram

Telegram is instant messaging service enabling users to send messages, photos, videos, stickers and files. Telegram describes itself as fast and secure solution for instant messaging and claims to be safer than WhatsApp. Compared to WhatsApp, Telegram is more cloud-based, it stores all messages on its servers and sync them with all user's devices.[19]

Nikolaj and Pavel Durov are the authors of Telegram. After leaving the social network VK Pavel Durov founded, they focused on creating safe forms of communication leading to Telegram.

Telegram provides two modes of messaging. Besides the regular chat Telegram provides "secret chats". Secret chat messages are encrypted using end-to-end encryption and are not stored on Telegram's servers[19].

Similar to WhatsApp user can contact someone using his phone number but Telegram provides classical username approach as well. User needs to know the reciepent's phone number or Telegram username in order to communicate with him.

All clients are licensed under GPLv2 or GPLv3 license, the server-side part of Telegram is closed-sourced and proprietery [20].

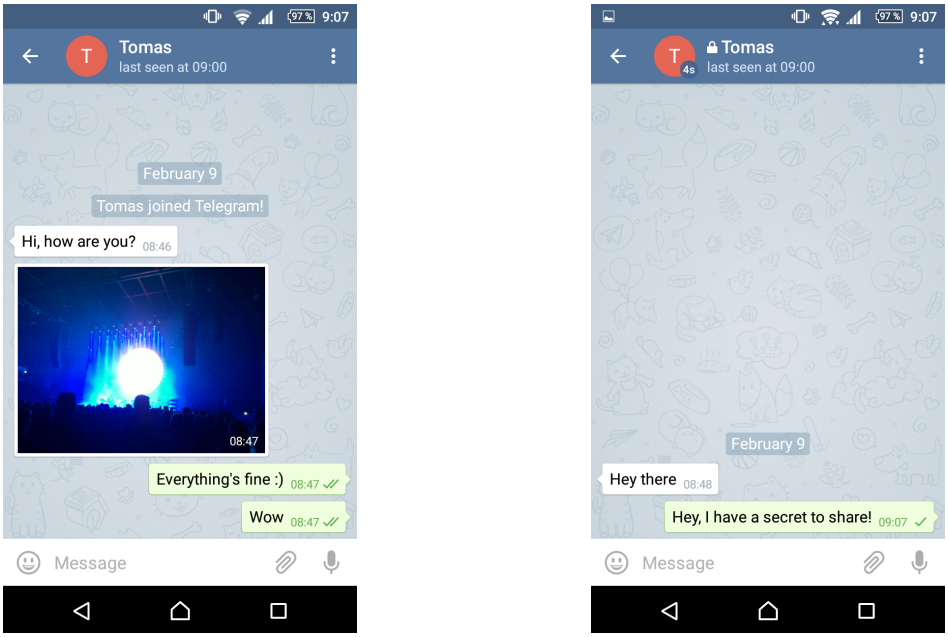
In 2015 Brazilian judiciary ordered WhatsApp to shut down for 48 hours. During this event, which was finally lowered to only 12 hours, Telegram welcomed 5 million new users.[21] It may be therefore considered as a direct competitor to WhatsApp.[10]

In May 2015 Telegram had 62 million active users [22].

1.4.1 Security-related incidents

Telegram was first released on August 14, 2013. The security-related history is thus not as broad as WhatsApp's.

[10]Tohle je spíš taková zajímavost, tak si nejsem úplně jist na kolik to sem patří



(a) Regular chat (b) Secret chat

Figure 1.3: Telegram chat modes

1.4.1.1 Possibly unsafe fundamentals

Telegram authors decided to create a brand new encryption scheme called MTProto. In cryptography community this raised concerns and some commented the approach as "*not something that a cryptographer would use*"[23]. Some of the alleged imperfections are:

- Telegram uses SHA-1 which is proven to be cryptographically broken [24].
- Telegram's authentication scheme is based on MAC-then-Encrypt approach instead of Encrypt-then-MAC.
- It uses IGE[11] mode in the AES encryption which is not well known. [12]

Telegram FAQ contradicts it uses the primitives in a safe manner [25].

1.4.1.2 IND-CCA insecurity

In Spring 2015 researchers from Aarhus University performed an independent audit of the protocol [26]. They concluded the encryption scheme is not IND-

[11] Infinite Garble Extension

[12] Pokud bych dělal Telegram, tohle je něco co by stálo za prozkoumání? Něco podobného útoku Padding Oracle. Prozkoumat ten IGE a tu autentikaci.

CCA[13] secure, meaning any ciphertext can be altered into another ciphertext decrypting to the very same plaintext.

The researchers stressed the theoretical nature of the attack and that they "*do not see any way of turning the attack into a full plaintext-recovery attack*"[26]. Telegram's FAQ describes it as a minor issue unaffecting overall security. [25]

1.4.1.3 Secret chat and Man-in-the-Middle attack

The secret chat provides an option to display counterparty's encryption key. Telegram creates a white-blue box to visualise the key as may be seen on 1.4. To make sure no malicious mediator is present users are supposed to meet in person and verify the keys are identical.

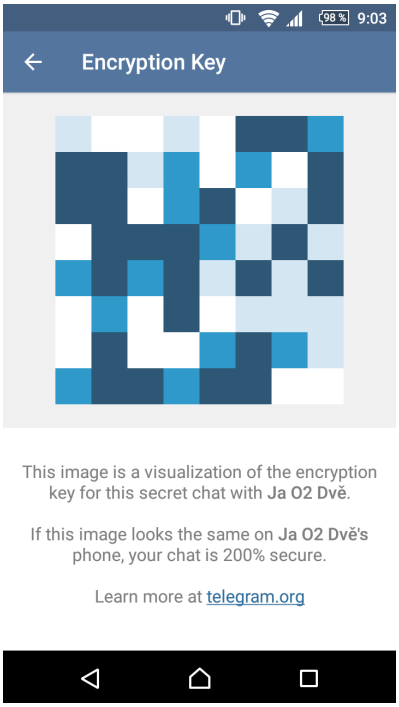


Figure 1.4: Encryption key visualisation

The visualisation is based on a 128-bit fingerprint of the secret key. An article presented in January 2015 showed[27] that when the attacker forces (e.g. socially engineers) both sides to initiate the secret chat, a MiM attack is possible only with 2^{64} operations, rather than 2^{128}, based on the birthday paradox.[14]

[13] Indistinguishability under Chosen Ciphertext

[14] Nevím, jestli bych to měl rozepsat nějak více. Ten článek není nijak skvělý, možná stačí později, jen v případě, že si telegram vyberu?

The article claims the attack is possible for a well financed adversary and estimates the attack to cost tens of millions USD. Telegram's FAQ addresses this issue and claimes its cost is around a trillion dollars to achieve a result in one month [25].

The article as well reasons that in real-world scenario the users don't meet up to verify the key. Most of them probably ignore the verification completely, some send the image via regular chat or using another channel.

1.4.1.4 Cracking Contest

On November 4, 2014, Telegram published contest with a winning price $300,000 for cracking its encryption. The contest became quite known in the community and probably provided a bit of advertisiment for Telegram.

The contest remained unsolved until his closure. Number of authors considered it rigged and stated that the contest does not provide any prove of Telegram's overall security whatsoever.[28][29]

1.4.2 EFF's secure messaging score

As mentioned Telegram has two types of messages. Telegram is therefore evaluated twice by the EFF.

1.4.2.1 Telegram regular chats

Table 1.3: Telegram regular chat's secure messaging score

Are messages encrypted in transit?	✓
Are messages encrypted so the provider can not access it?	✗
Can user verify contacts' identities?	✗
Are past communications secure if keys stolen?	✗
Is the code open to independent review?	✗
Is the cryptography design properly documented?	✓
Has there been any recent code audit?	✓

1.4.2.2 Telegram secret chats

1.5 Signal

Signal is a voice calling and instant messaging application developped by Open Whisper Systems. It was brought to light by the merge of two applications – the voice calling RedPhone and the text messenger TextSecure both created by the very same company [30].

Table 1.4: Telegram secret chat's secure messaging score

Are messages encrypted in transit?	✓
Are messages encrypted so the provider can not access it?	✓
Can user verify contacts' identities?	✓
Are past communications secure if keys stolen?	✓
Is the code open to independent review?	✓
Is the cryptography design properly documented?	✓
Has there been any recent code audit?	✓

Signal is completely open-sourced including its server side. Signal was endorsed by some well-known names such as Edward Snowden [31] or Bruce Schneier [32].

TODO

1.5.1 EFF's secure messaging score

Table 1.5: Signal's secure messaging score

Are messages encrypted in transit?	✓
Are messages encrypted so the provider can not access it?	✓
Can user verify contacts' identities?	✓
Are past communications secure if keys stolen?	✓
Is the code open to independent review?	✓
Is the cryptography design properly documented?	✓
Has there been any recent code audit?	✓

1.6 Threema

TODO napsat cenu

Threema is paid proprietary instant messaging application. Users can send photos, videos, voice messages, QR codes, polls and files [33]. TODO: citovani homepage?

It provides end-to-end encryption and claims to prevent collection of any metadata [33].

Threema does not use phone numbers or usernames. It generates a random ID for user identification. Phone number and email are not required, no personal information are therefore needed.

As of June 2015, Threema had 3.5 million active users, mostly in german-speaking countries.[34]

1.7 WeChat

WeChat is properietary application. It was released in January 2011 and allows users to send text messages, voice messages, communicate via phone or video calls, it provides location sharing functions and other various functions [35].

As of August 2015, WeChat has 600 million active users, vast majority of them located in China.[36]

Conclusion

Zaver TODO

Bibliography

[1] djwm. *Sniffer tool displays other people's WhatsApp messages* [online]. May 2012, [accessed 2016-02-02]. Available from: http://www.h-online.com/security/news/item/Sniffer-tool-displays-other-people-s-WhatsApp-messages-1574382.html

[2] BBC. *WhatsApp reaches a billion monthly users* [online]. Feb. 2016, [accessed 2016-02-02]. Available from: http://www.bbc.com/news/technology-35459812

[3] Covert, A. *Facebook buys WhatsApp for $19 billion* [online]. Feb. 2014, [accessed 2016-01-26]. Available from: http://money.cnn.com/2014/02/19/technology/social/facebook-whatsapp/

[4] Electronic Frontier Foundation. *Secure Messaging Scorecard* [online]. [accessed 2016-02-02]. Available from: https://www.eff.org/secure-messaging-scorecard

[5] WhatsApp. *WhatsApp homepage* [online]. Jan. 2016, [accessed 2016-01-26]. Available from: https://www.whatsapp.com/?l=en

[6] Kurtz, A. *Shooting the Messenger* [online]. Sept. 2011, [accessed 2016-01-31]. Available from: http://www.andreas-kurtz.de/2011/09/shooting-messenger.html

[7] Gevers, R. *Hijack Whatsapp with your iPhone* [online]. Sept. 2011, [accessed 2016-01-31]. Available from: http://rickey-g.blogspot.com/2011/05/hijack-someone-elses-whatsapp-with-your.html

[8] mgp25. *WhatsApp Protocol - FunXMPP* [online]. Dec. 2014, [accessed 2016-01-31]. Available from: https://github.com/mgp25/Chat-API/wiki/FunXMPP-Protocol

[9] Heckel, P. C. *How To: Sniff the WhatsApp password from your Android phone or iPhone* [online]. July 2013, [accessed 2016-01-31]. Available from: https://blog.heckel.xyz/2013/07/05/how-to-sniff-the-whatsapp-password-from-your-android-phone-or-iphone/

[10] Damania, D. *Use Whatsapp? You Phone number is your Username and IMEI is the password – Hackable* [online]. Sept. 2012, [accessed 2016-01-31]. Available from: http://thednetworks.com/2012/09/09/whatsapp-imei-password-md5-inverted-hack/

[11] Yourdailymac. *WhatsApp leaks usernames, telephone numbers and messages* [online]. May 2011, [accessed 2016-02-02]. Available from: http://www.yourdailymac.net/2011/05/whatsapp-leaks-usernames-telephone-numbers-and-messages/

[12] Summerson, C. *WhatsAppSniffer Shames WhatsApp's Plaintext, Unprotected Chat Transfer Protocol, Shows Off Just How Much Can Be Sniffed* [online]. May 2012, [accessed 2016-02-02]. Available from: http://www.androidpolice.com/2012/05/02/whatsappsniffer-shames-whatsapps-plaintext-unprotected-chat-transfer-protocol-shows-off-just-how-much-can-be-sniffed/

[13] fab. *WhatsApp no longer sends plain text* [online]. Aug. 2012, [accessed 2016-02-02]. Available from: http://www.h-online.com/security/news/item/WhatsApp-no-longer-sends-plain-text-1674723.html

[14] Alkemade, T. *Piercing Through WhatsApp's Encryption* [online]. Oct. 2013, [accessed 2016-02-02]. Available from: https://blog.thijsalkema.de/blog/2013/10/08/piercing-through-whatsapp-s-encryption/

[15] Brewster, T. *WhatsApp Users 'Should Not Trust Broken Encryption'* [online]. Oct. 2013, [accessed 2016-02-02]. Available from: http://www.techweekeurope.co.uk/workspace/whatsapp-encryption-security-128964

[16] Marlinspike, M. *Open Whisper Systems partners with WhatsApp to provide end-to-end encryption* [online]. Nov. 2014, [accessed 2016-01-26]. Available from: https://whispersystems.org/blog/whatsapp/

[17] WhatsApp. *WhatsApp FAQ* [online]. [accessed 2016-02-02]. Available from: https://www.whatsapp.com/faq/en/general/21864047

[18] Scherschel, F. *Keeping Tabs on WhatsApp's Encryption* [online]. Apr. 2015, [accessed 2016-02-02]. Available from: http://www.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html

[19] Telegram. *Telegram FAQ* [online]. [accessed 2016-01-26]. Available from: https://telegram.org/faq

[20] Petrielli, P. *Telegram Messenger: Review* [online]. July 2015, [accessed 2016-02-02]. Available from: http://techglobule.com/2015/07/telegram-messenger/

[21] Ruvolo, J. *Brazilian Judge Shuts Down WhatsApp And Brazil's Congress Wants To Shut Down The Social Web* [online]. Dec. 2015, [accessed 2016-01-26]. Available from: http://www.techcrunch.com/2015/12/16/brazils-congress-has-shut-down-whatsapp-tonight-and-the-rest-of-the-social-web-could-be-next

[22] Savov, V. *Brazil's WhatsApp ban is driving millions of users to Telegram* [online]. Dec. 2015, [accessed 2016-02-02]. Available from: http://www.theverge.com/2015/12/17/10386776/brazil-whatsapp-ban-telegram-millions-users

[23] Savov, V. *Cryptography expert casts doubt on encryption in ISIS' favorite messaging app* [online]. Nov. 2015, [accessed 2016-02-07]. Available from: http://www.dailydot.com/politics/telegram-isis-encryption-cryptography/

[24] Schneier, B. *SHA-1 Broken* [online]. Feb. 2005, [accessed 2016-02-09]. Available from: https://www.schneier.com/blog/archives/2005/02/sha1_broken.html

[25] Telegram. *FAQ for the Technically Inclined* [online]. [accessed 2016-02-07]. Available from: https://telegram.org/faq

[26] Jakobsen, J. B. A practical cryptanalysis of the Telegram messaging protocol *[online]*. Master's thesis, Aarhus University, Sept. 2015. Available from: http://cs.au.dk/~jakjak/master-thesis.pdf

[27] adc. *A $2^6$4 Attack On Telegram, And Why A Super Villain Doesn't Need It To Read Your Telegram Chats.* [online]. Jan. 2015, [accessed 2016-02-09]. Available from: http://www.alexrad.me/discourse/a-264-attack-on-telegram-and-why-a-super-villain-doesnt-need-it-to-read-your-telegram-chats.html

[28] Marlinspike, M. *A Crypto Challenge For The Telegram Developers* [online]. Dec. 2013, [accessed 2016-01-26]. Available from: http://thoughtcrime.org/blog/telegram-crypto-challenge/

[29] Crypto Fails. *Telegram's Cryptanalysis Contest* [online]. Dec. 2013, [accessed 2016-01-26]. Available from: http://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest

[30] Marlinspike, M. *Just Signal* [online]. Nov. 2015, [accessed 2016-01-26]. Available from: https://whispersystems.org/blog/just-signal/

[31] McCormick, R. *Edward Snowden's favorite encrypted chat app is now on Android* [online]. Nov. 2015, [accessed 2016-02-10]. Available from: http://www.theverge.com/2015/11/3/9662724/signal-encrypted-chat-app-android-edward-snowden

[32] Schneier, B. *Testing the Usability of PGP Encryption Tools* [online]. Nov. 2015, [accessed 2016-02-10]. Available from: https://www.schneier.com/blog/archives/2015/11/testing_the_usa.html

[33] Price, R. *Germany's most popular paid app is a secure messenger loved by millions – now it's taking on the US* [online]. June 2015, [accessed 2016-01-26]. Available from: http://uk.businessinsider.com/threema-encryption-messaging-app-america-launch-isis-2015-6

[34] Threema. *Threema homepage* [online]. [accessed 2016-01-26]. Available from: https://threema.ch/en

[35] WeChat. *WeChat homepage* [online]. [accessed 2016-01-26]. Available from: http://www.wechat.com/en/features.html

[36] Lee, E. *WeChat Marked 600 Million Monthly Active Users, Up 37% YOY* [online]. Aug. 2015, [accessed 2016-01-26]. Available from: http://technode.com/2015/08/14/wechat-600m-mau/

Appendix A

Contents of CD

Visualise the contents of enclosed media. Use of `dirtree` is recommended. Note that directories src and text with appropriate contents are mandatory.

```
readme.txt ..... the file with CD contents description
data ..... the data files directory
    graphs ..... the directory of graphs of experiments
        *.eps ..... the B/W graphs
        *.png ..... the color g¡raphs
        *.dat ..... the graphs data files
exe ..... the directory with executable WBDCM program
    wbdcm ..... the WBDCM program executable (UNIX)
    wbdcm.exe ..... the WBDCM program executable (Windows)
src ..... the directory of source codes
    wbdcm ..... the directory of WBDCM program
        Makefile ..... the makefile of WBDCM program (UNIX)
    thesis ..... the directory of LaTeX source codes of the thesis
        figures ..... the thesis figures directory
        *.tex ..... the LaTeX source code files of the thesis
text ..... the thesis text directory
    thesis.pdf ..... the Diploma thesis in PDF format
    thesis.ps ..... the Diploma thesis in PS format
```