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

2nd February 2016

TODO

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 2nd 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. The selection is based on criteria such as user base, license and overall security it claims to provide [1]. [2]

Table 1.1: Messengers

Name	**Authors**	**First realease**	**License**	**User b**
WhatsApp	WhatsApp Inc.	January 2010	Proprietary	990 mil
Telegram	Telegram Messenger LLP	August 2013	GPLv2/GPLv3/Properietary[4]	60 milli
Signal	Open Whisper Systems	July 2014	GPLv3	10 milli
Threema	Threema GmbH	December 2012	Proprietary	3.5 mill
WeChat	Tencent	January 2011	Proprietary	600 mil

The Electronic Frontier Foundation maintains a scoreboard of messaging applications' security. It evaluates messengers based on these seven criteria [2]:

- Are messages encrypted in transit?
- Are messages encrypted so the provider can't read it?
- Can user verify contacts' identities?

[1] Více rozepsat?

[2] Napsat proč tu není Facebook Messenger anebo ho přidat

[3] As of September 2015.

[4] Rozepsat? Serverová verze je closed-source.

[5] As of September 2015.

[6] *Predchudce a As of December 2013. Ma smysl porovnavat, kdyz je to 2 roky stare?

[7] As of June 2015.

[8] As of August 2015.

- Are past communications secure if keys stolen?
- Is the code open to independent review?
- Is security design properly documented?
- Has there been any recent code audit?

At the end of each chapter dedicated to one messenger a small note about the received score is present.

1.1 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 Nokia[3].

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

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

WhatsApp Messenger is a proprietary software, currently own by Facebook Inc [4]. Becuase of that fact, the writer decided to omit Facebook Messenger, since it resembles WhatsApp closely[9].

Following section describes WhatsApp's security-related incidents and an attitude to its security in general.

1.1.1 Security-related incidents

1.1.1.1 Flaws in registration process

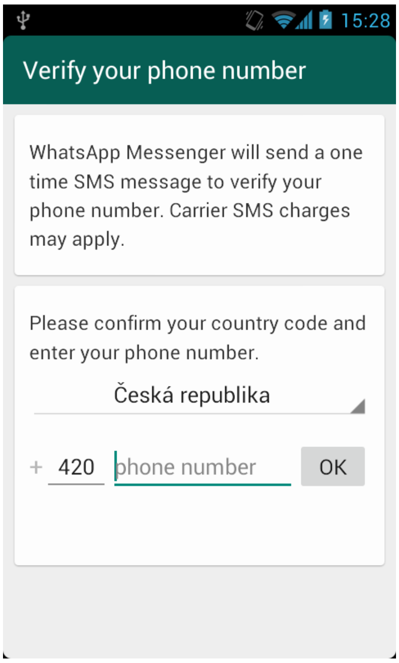
WhatsApp's user identity is bound to user's phone number. In order to verify the relationship user has to enter his phone number during the first start-up. WhatsApp server then sends SMS with verification code to such number. User submits the code from the received text message and WhatsApp creates his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

Older versions of 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 [5].

In 2011 research showed this method had serious drawbacks. To hijack user's account attacker first opted for this method. Then using SMS spoofing service[10] he sent SMS to WhatsApp's phone number pretending it originates

[9] Tohle je pravda tak napůl

[10] popsat co to je, nebo není třeba?



15:28

Verify your phone number

WhatsApp Messenger will send a one time SMS message to verify your phone number. Carrier SMS charges may apply.

Please confirm your country code and enter your phone number.

Česká republika

+ 420 phone number OK

Figure 1.1: WhatsApp's registration process

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 [6].

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 [5]:

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[11], 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

[11] Přidat poznámku o HTTP/HTTPS a zachycení requestu?

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 [5].

To the date of writing this thesis WhatsApp doesn't offer discussed verification method anymore.

1.1.1.2 Password generation

WhatsApp uses lightly modified version of XMPP [7]. During the registration process it creates a username based on the user's phone number. In newer versions of the client the password is generated on server's side [8]. However, the previous Android versions used the phone's IMEI number as password [8][9].

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.

1.1.1.3 Messages encryption

In former versions, 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 [10]. Using a simple network sniffer like Wireshark attacker was able to read all user's messages [10].

On May 2012 an application called "WhatsAppSniffer" had been released. It abused described flaw and enabled attacker to see victim's messages in easy and lucid user interface [11][12].[12]

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].

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 [16]. Open Whisper Systems stated: *"we are moving quickly towards a world where all WhatsApp users will get end-to-end encryption by default."* [16].

[12] dodat obrazek?

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 [18].

1.1.1.4 APIs

[13]

1.1.1.5 EFF's secure messaging score

At the time of writing WhatsApp has two points out of seven in the EFF's secure messaging scorecard [2].

1.2 Telegram

Telegram is instant messaging service, enabling users to send messages, photos, videos, stickers and files. It was first released on August 14, 2013[19]. Telegram describes itself as fast and secure solution for instant messaging [19] and claims to be safer than WhatsApp[19]. Compared to WhatsApp, Telegram is more cloud-based, it stores all messages on its servers and sync them with all user's devices [19].

Similar to WhatsApp user can contact someone by his phone number. 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, however the server-side part of Telegram is closed-sourced and proprietery. TODO overit

In 2015 Brazilian judiciary ordered WhatsApp to shut down for 48 hours [20]. During this event, which was finally lowered to only 12 hours, Telegram welcomed 5 million new users [20]. It may be therefore considered as a direct competitor to WhatsApp.

In September 2015, Telegram officials stated announced it has 60 million active users.[**?**]

[13] Napsat o Chat API a WhatsAPI?

1.2.1 Secret chats

Besides 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].

1.2.2 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 as rigged and stated that the contest does not provide any prove of Telegram’s overall security whatsoever.[21][22]

1.2.3 MTProto protocol

Telegram uses its own encryption protocol called MTProto. One of the basic rules of cryptography is not to “roll your own crypto”.

TODO popsat celý protokol?

1.3 Signal

Signal is a voice calling and instant messaging application developped by Open Whisper Systems. It was brought to light by merging two applications - the voice calling RedPhone and the text messenger TextSecure both created by the very same company [23].

Signal is completely open-sourced including its server side.

TODO

1.4 Threema

Threema is paid proprietary instant messaging application. Users can send photos, videos, voice messages, QR codes, polls and files [24]. TODO: citovani homepage?

It provides end-to-end encryption and claims to prevent collection of any metadata [24].

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.[25]

1.5 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 [26].

As of August 2015, WeChat has 600 million active users, vast majority of them located in China.[27]

Conclusion

Zaver TODO

Bibliography

[1] BBC. *bbc.com* [online]. Feb. 2016, [accessed 2016-02-02]. Available from: `http://www.bbc.com/news/technology-35459812`

[2] Scorecard, E. S. M. *eff.org* [online]. [accessed 2016-02-02]. Available from: `https://www.eff.org/secure-messaging-scorecard`

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

[4] CNN. *money.cnn.com* [online]. Feb. 2014, [accessed 2016-01-26]. Available from: `http://money.cnn.com/2014/02/19/technology/social/facebook-whatsapp/`

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

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

[7] Protocol, C. A. F. *github.com/mgp25/Chat-API* [online]. Dec. 2014, [accessed 2016-01-31]. Available from: `https://github.com/mgp25/Chat-API/wiki/FunXMPP-Protocol`

[8] Heckel, P. C. *heckel.xyz* [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/`

[9] Damania, D. *thednetworks.com* [online]. Sept. 2012, [accessed 2016-01-31]. Available from: `http://thednetworks.com/2012/09/09/whatsapp-imei-password-md5-inverted-hack/`

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

[11] Summerson, C. *androidpolice.com* [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/`

[12] H, T. *h-online.com* [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`

[13] H, T. *h-online.com* [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. *blog.thijsalkema.de* [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. *techweekeurope.co.uk* [online]. Oct. 2013, [accessed 2016-02-02]. Available from: `http://www.techweekeurope.co.uk/workspace/whatsapp-encryption-security-128964`

[16] Open Whisper Systems. *whispersystems.org* [online]. Nov. 2014, [accessed 2016-01-26]. Available from: `https://whispersystems.org/blog/whatsapp/`

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

[18] Scherschel, F. *heise.de* [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.org* [online]. [accessed 2016-01-26]. Available from: `https://telegram.org/faq`

[20] TechCrunch. *techcrunch.com* [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`

[21] Marlinspike, M. *thoughtcrime.org* [online]. Dec. 2013, [accessed 2016-01-26]. Available from: `http://thoughtcrime.org/blog/telegram-crypto-challenge/`

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

[23] Open Whisper Systems. *whispersystems.org* [online]. Nov. 2015, [accessed 2016-01-26]. Available from: https://whispersystems.org/blog/just-signal/

[24] Business Insider UK. *uk.businessinsider.com* [online]. June 2015, [accessed 2016-01-26]. Available from: http://uk.businessinsider.com/threema-encryption-messaging-app-america-launch-isis-2015-6

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

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

[27] technode. *technode.com* [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 graphs
    *.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
```