Daria Nurtdinova

SECURITY IN MOBILE MESSAGING

Bachelor's Thesis
Information Technology

April 2016

MAMK
University of Applied Sciences

DESCRIPTION

MAMK
University of Applied Sciences

Date of the bachelor's thesis

6 May 2016

Author(s)

Daria Nurtdinova

Degree programme and option

Information Technology

Name of the bachelor's thesis

Security in mobile messaging

Abstract

Nowadays the Internet and smartphones are a substantial part of everyday life. It helps us to be in touch with others and to manage business projects more easily. IM immediately adapts to the possibilities of digital sphere and to human requirements. The academic purpose is to review the development of messaging applications and security features through the last 25 years.

The main aim of the case is to find a free of charge cross-platform instant messenger with the end-to-end encrypted connection. The chosen app with a new security policy gradually introduces and implements better data protection for the case company. Methods include data collection, analyze, testing and weighed score comparison.

It is not possible to secure users, data or devices from every threat. However, it is possible to reduce risk in dozens of times by implementing basic configurations. The level of use and understanding of the technology among various groups varies considerably, so user-friendly communication software makes employees accustomed with encrypted communication concept. Further development for the case company involves improving smartphones security including passwords, antiviruses, and monitoring application.

This study highlights that development in Internet applications sphere goes very fast and thigs changes frequently. It is important to review security of the system continuously.

Subject headings, (keywords)

Instant messaging, security

Pages	**Language**	**URN**
51	English	

Remarks, Notes on appendices

Tutor	**Bachelor's thesis assigned by**
Matti Koivisto	Mikkeli University of Applied Sciences

CONTENTS

VOCABULARY

DDoS – Distributed Denial of Service – attack to overflood the system with requests

XMPP – Extensible Messaging and Presence Protocol – communication protocol for near-real-time data exchange including text messages, VoIP, video, file sharing, gaming

VoIP –Voice over IP – transmission of voice data over Internet Protocol networks

IM – instant messaging – real-time communication online using text

ID – Identifier – a unique symbol set for authentication and recognition in a system

IRC – Internet Relay Chat – transfer protocol for text messaging online

WEP – Wired Equivalent Privacy – security algorithm for wireless network

WPA – Wi-Fi Protected Access – wireless encryption standard

TKIP – Temporal Key Integrity Protocol – encryption algorithm for wireless networks

BSSID – Basis Service Set Identification – wireless access point identification in LAN

IPS - Intrusion Prevention System – security tool that monitor and halt malicious activity in the system

P2PP – Peer-to-Peer Protocol – protocol on application layer between network members

MiTM – Man in the middle – attack when the third party can access, read and change messages while received messages seem to be legitimate and correct

ROM – Read-only memory – memory which keeps data even without power

LAN – Local Area Network – computers connected in a small area like office

HTTP – Hypertext Transfer Protocol – application protocol to exchange web pages and other data files over the Internet

SMS – Short Message Service – text only messaging on mobile phones

MMS – Multimedia Messaging Service – messaging communication on cell phones allowing video, animation, image, audio or text exchange

IMSI – International Mobile Subscriber Identity – cellular network user ID

UX – user experience – person's attitudes and behavior using a specific product

NSA – National Security Agency – USA intelligence organization

E2EE – End-to-end encryption – uninterrupted data protection between two parties with no third-party access

PC – personal computer – computer for individuals

OS – operating system – system software that manages computer resources and provides common services

CIA – Confidentiality, Integrity, Availability – model of guiding information security policies

1 INTRODUCTION

The Internet, as well as other communication media like a telephone, changed the way information is spread, processed, and influenced. The Internet makes new models of human interactions possible through instant messaging, Internet forums, and social networking. There is no centralized consolidate administration like government in any technological implantations which will control access and the use of data. Networks set their rules and policies. Nevertheless, in the USA only, there are over 10 000 regulations related to digital messaging, electronic communication and records confinement (Enterprise Storage Group, 2003).

There are more smartphones with access to the Internet than computers, though this is not so broadly known. Global mobile penetration reached 100% at the end of 2015. Roughly speaking, there is a SIM card per each human on the planet. (Talmesio, 2016). Overall Internet usage has seen tremendous growth. The Internet's technologies have advanced plenty in recent years. The use of Unicode, particularly, provides ease of communication not only in languages using Latin letters but the world's languages including hieroglyphics for example. People use messaging to make friends worldwide and to stay in touch with them.

Social network services, e.g. Facebook, MySpace, Tumblr, and Twitter, establish new interaction models. There are special websites and social networks. For example, LinkedIn for business connections, YouTube for sharing videos, Flickr and Instagram for photos sharing. Instant messaging created an advanced way of casual, simple communication for people that have impairment in hearing or an auditory or speech disability. It is an efficient form that grants equal opportunities for communication, without the support of special devices or services created for users with hearing loss.

The need to regulate Internet access has the same root as equal opportunities for people with disabilities, because children can face dangers online. Children have a chance of discovering material which they might find disturbing or upsetting, or information which their parents find not age-appropriate. Due to inexperience, naivety and lack of knowledge, children may spread personal information about themselves on the Internet. This could bring risks toward them or their families. It is important to warn children about the consequences in time. Parents frequently choose to turn on Internet filtering

and control their children's online activities in an effort to guard their children from unsuitable information. Popular social networks, e.g. Facebook and Twitter, ordinarily deny account registration under the age of 13. However, such policies are commonly insignificant to bypass by registering with a fake ID, and a serious number of children under 13 years old join desirable websites anyhow. There are also social networks designed especially for young children which affirm to arrange improved levels of safety (Kessler, 2010). Nevertheless, at some moment, children refer such web pages as with no interest for them.

There are vulnerabilities for both individuals' and organizations' posting, primarily public posts, on social networks and blogs. This is especially related to absurd or disputed and questionable text that occasionally start an astonishing and probably enormous reaction on social media from other Internet users. Moreover, widely known than such reaction brings even more risks when transited in real world action, e.g. demonstrations, damage of property. There are websites, e.g. Reddit, that set rules to prohibit the posting of persons' private information – doxxing. The reason is that doxxing leads to mobs of massive numbers of users sending harassment to that particular person thereby identified.

This thesis involves both theoretical and practical aims. The academic purpose is to review the development of messaging applications and also security features through the last 25 years. The practical purpose is to find and compare the most secure, user-friendly cross-platform messengers for a case company. It is preferable to have a different way to communicate and to send files through a messenger in the local network and through the Internet.

Chapter 2 covers the history of the development of messengers and the most popular and secure messengers. Chapter 3 explores security vulnerabilities and protective solutions. Chapter 4 will unite my study with a Company case and collect data. Chapter 5 is about choosing appropriate software. The last Chapter 6 introduces conclusions, the limitations of the study and further development ideas.

2 HISTORY OF MESSAGING AND ITS DEVELOPMENT

Instant messaging, or shortly IM, is an efficient way of communication in case of physical barriers when people cannot talk directly to each other. Since the middle of the 1990s PC and Internet connection became available to a larger number of people. By this time, near-instant communication has had a drastic effect on communication culture. It includes instant messaging, email, VoIP, video conferencing as well as blogs, forums and social networks in the World Wide Web.

2.1 Emergence of computer messaging: 1970–2000

Instant messaging is an exchange of text on online chat or other software in real-time. Instant messaging services come from Internet Relay Chat, early instant messaging programs, where a symbol appeared while typed and was seen both by author and reader. Then letters were removed to correct typographical errors. Screenshot can be seen in Figure 1.

Applications for instant messaging began to appear in the 1970s. Firstly on multi-user operating systems like UNIX, originally to facilitate communication with other users logged in at first to the same host, then local network, and finally across the world wide net. There are two types of IM: peer-to-peer protocol, used for example in the talk, ytalk and ntalk, and server-based where peers connect to a server, e.g. talker, IRC.

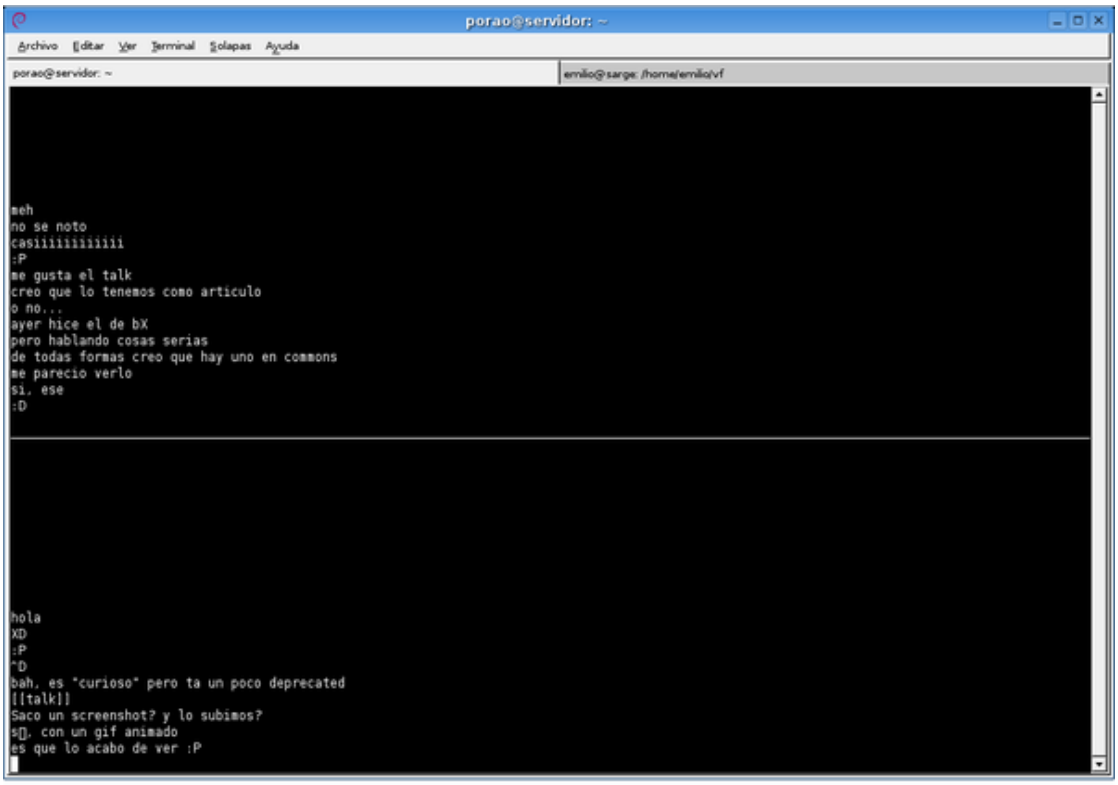


FIGURE 1. Command-line Unix program talk with a split screen user interface (Usuario:Porao, 2006)

In August 1982, the Quantum Link online service for Commodore nb64 computers made available peer-to-peer messages via the PETSCII system. The screen was visually split into sections. On the top of the screen messages appear as a yellow bar saying ‘Message From:’ with the sender’s nickname forwarded with the message. The bottom part had a list of respond options as some kind of a prototype for today’s push notifications (On-Line Messages can be seen in Figure 2). On-Line Messages were an extra service above the monthly Q-Link access costs, meaning there was an additional per-minute fee. (Hoyos, 2008)

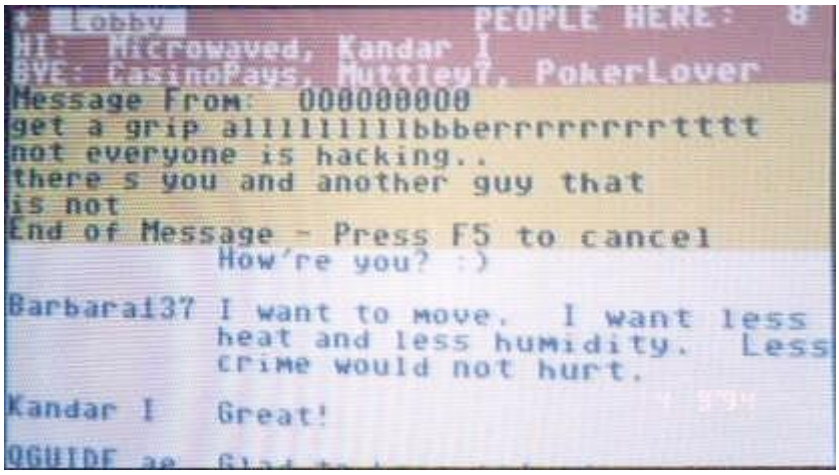


FIGURE 2. On-Line Messages system on Commodore nb64 (qlinklives.org, 2007)

In 1983 high school student Mark Jenks built an instant messenger named talk. It allowed private messaging, social networking rooms and bulletin boards among Washington High School students by login into the system with a screenname or handle (Hoyos, 2008). In August 1988 Jarkko Oikarinen created Internet Relay Chat which gave users opportunity to send private messages, as well as allowed multi-user groups named channels and file sharing over a data transport system (Oikarinen, 2010). In October 1991 Quantum Link's more commonly known embodiment America OnLine started developing an analogous product named AOL Instant Messages, which was presented in May 1997, with IM, chat rooms and file sharing (Abbruzzese, 2014).

Current Internet-wide messaging clients with a graphical user interface, as they are known now, started off in the middle of the 1990s. Well-known examples are ICQ, shown in Figure 3, followed by AOL Instant Messenger in 1997 (riko, 2009). Mirabilis, the creator of ICQ, was later acquired by AOL (Hansell, 1998). In 2002 ICQ under AOL patented two technologies for instant messaging by the US patent office. From now on, the term instant messenger is a Time Warner’s service mark and may not be used in software not connected with AOL in the United States (United States Patent and Trademark Office, 2006).

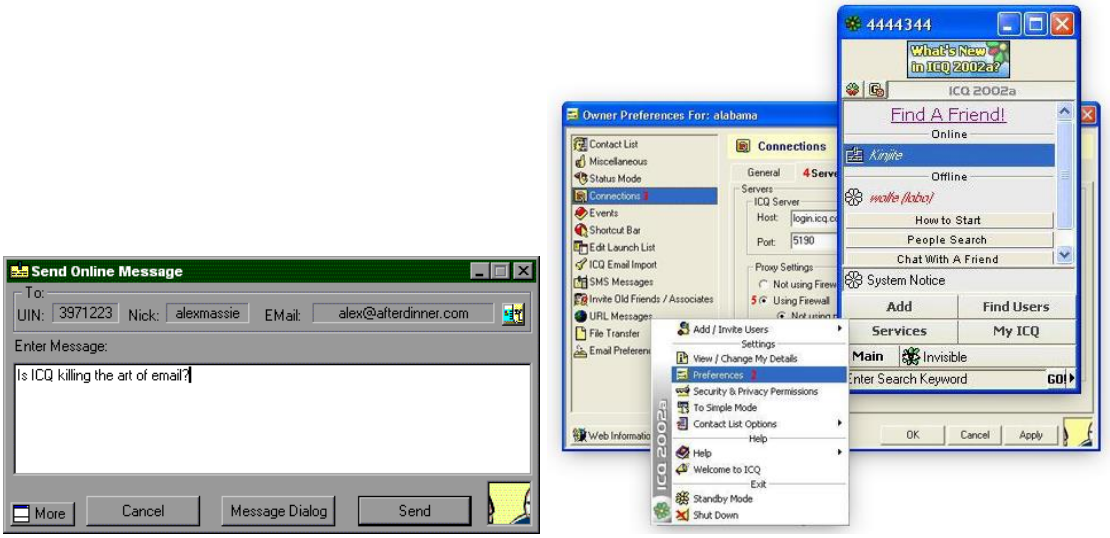


FIGURE 3. ICQ interface in 1997 and 2000 (Mail.Ru Group, 2015)

In 1998 Yahoo! launched Yahoo! Papers, an application for instant messaging with better security features, including profile personalization options and the ability to block unwanted contacts (Hoyos, 2008). At the same time, MSN in 1999, IBM, Ubique and others through the 2000s created their own proprietary protocols and IM clients. Therefore, users had to run numerous apps to communicate with each other (Abbruzzese, 2014).

In 2000 Jabber was launched. It is an open standards-based protocol and an open source program. Jabber servers act as gateways to other IM protocols, lowering the need to run multiple applications and allowing users to chat simultaneously with Yahoo!, MSN and the AIM contact list in a single application. The protocol was later standardized as XMPP. Popular in the 2000s instant messengers like Pidgin, Trillian, Gaim, Adium, and Miranda were multi-protocol clients without the necessity for a server gateway. Jabber on Gaim software can be seen in Figure 4.

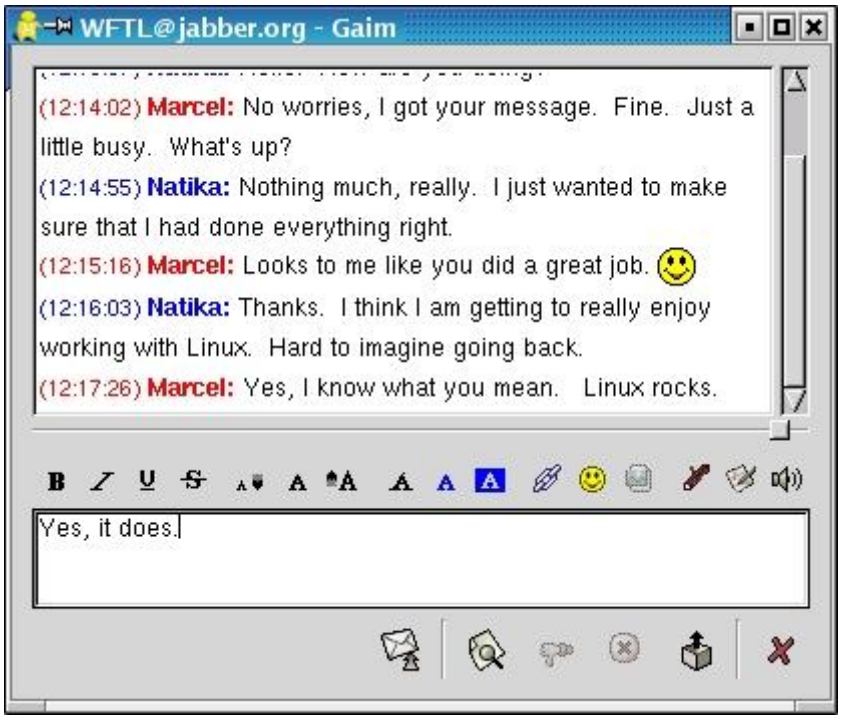


FIGURE 4. Jabber on Gaim, Linux IM software (Gagné, 2003)

2.2 The application shift from computers to mobile: 2000–2016

Mobile completes a journey from one computer on earth to a computer in literally every pocket. Moreover, mobile brings computing to people hardly touched by technology before. Today networks are available almost everywhere. The entry price for Android device is USD 35 – 50, although access to affordable data and power is the largest remaining barrier in the least developing countries. Mobile becomes the Internet – the main way that most people go online. Smartphones have much greater internet penetration (Evans, 2015), and as can be seen in Figure 5, mobile phones are more available than a personal computer.

Availability and therefore the popularity of smartphones give a second wind to instant messengers. There is a possibility to download an application on the mobile phone to communicate on-the-go in the corporate network, e.g. Reuters, Sametime, LCS, or public network, e.g. ICQ, Yahoo!, Google Talk, MSN, AIM. Among the benefits of using an IM client over SMS text messages are chat mode, group mode, fast delivery and quick response, file transfer and video conferencing. In addition, using the data communication is cheaper in most cases. In contrast to e-mail, IM allows showing status if a user is available, busy, away or showing offline status. According to GSMA (2016),

global SMS is 20 billion messages a day. At the same time, the popular IM application WhatsApp has 30 billion messages a day (WhatsApp Inc., 2016).

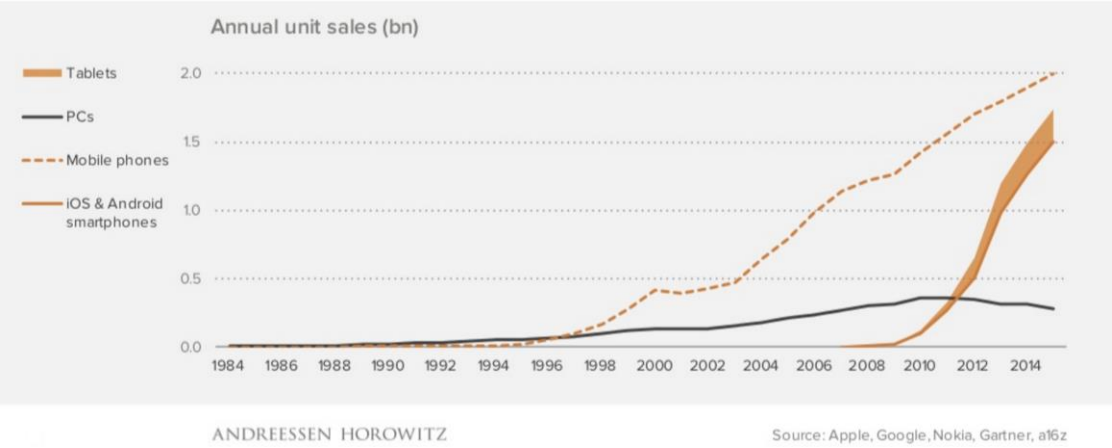


FIGURE 5. Comparison of PC and mobile devices annual sales (Evans, 2016)

One of the fundamental things that smartphones changed about the internet is that the smartphone itself is a social platform. Every app can access the user's address book, getting an instant social graph. The phone number, in particular, acts as a unique social identifier. The software can access the photo library and camera directly as well as location, making file sharing easy. Every app is just two taps away from the home screen, which makes switching between services easier and also drives a trend for focused, single-purpose apps over apps that do everything. It is easier to find a feature as an icon on home screen than as an option in a sub-menu of the program. (Evans, 2015)

Mobile is a unique ecosystem that differs from PC in 10x scale. Smartphones provide a native touch UX and secure sandboxed software model. Tablets and Chromebooks address to a personal computer but also come from a mobile ecosystem. This shows how mobile replace PC world. PC internet mostly meant searching and the web browsing. Mobile unbundles the web into apps. Apps cover over half of the Internet use (Comscore, 2015). This can be seen in Figure 6.

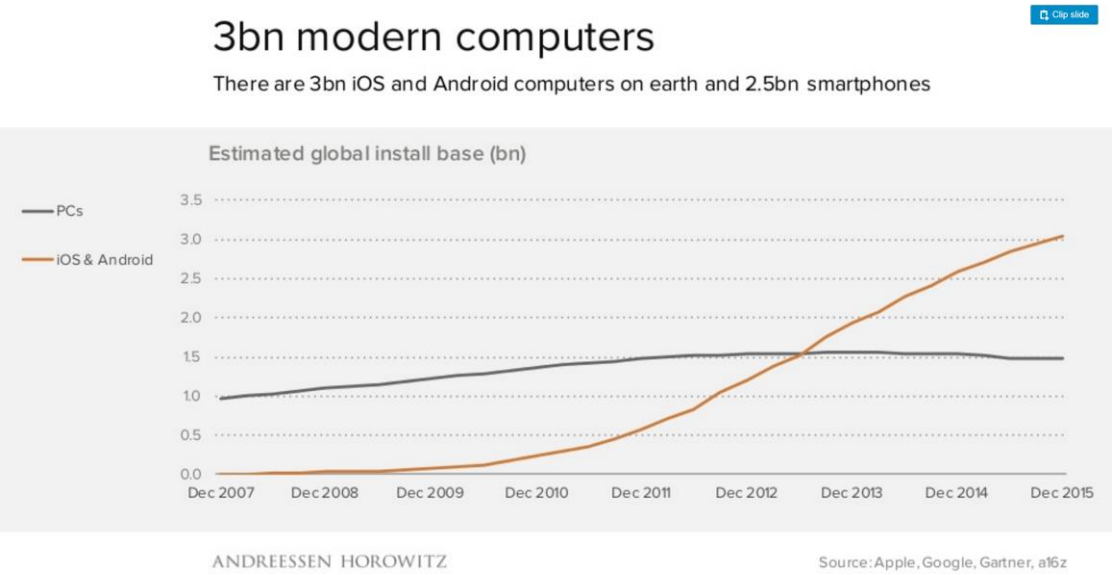


FIGURE 6. Number of PC and mobile devices global (Evans, 2016)

In the 2010s, IM was commonly provided by social networks. Almost every social application implemented some way of direct messages at least. Recently, IM provides not only text messaging but also voice, video, and file sharing features, followed further by web conferencing services. Web conferencing merges video and instant messaging capacity, e.g. in Skype. New features invented and popularized by IM apps are stickers and emoticons – detailed illustrations of emotions or actions. The usage of stickers allows another level of communication.

In January 2014, Strategy Analytics report that telecommunications operators' revenues from delivering SMS and MMS by the end of 2013 decreased for the first time in the history. Analysts predict that by 2017 revenues will be reduced by 20%. Meanwhile, the audience of messengers grows (Patel, 2014). In June 2015, Strategy Analytics update the prognoses to a 42% revenue decrease by 2021. The number of text messages sent each month is 350 billion, and the number of instant messages shared at the same time is 1.5 trillion, and growing rapidly (IBM Security, 2015).

2.3 Current messaging systems

Instant messengers' applications are usually divided into two categories: Consumer Instant Messaging (CIM) and Enterprise Instant Messaging (EIM). CIM covers free or

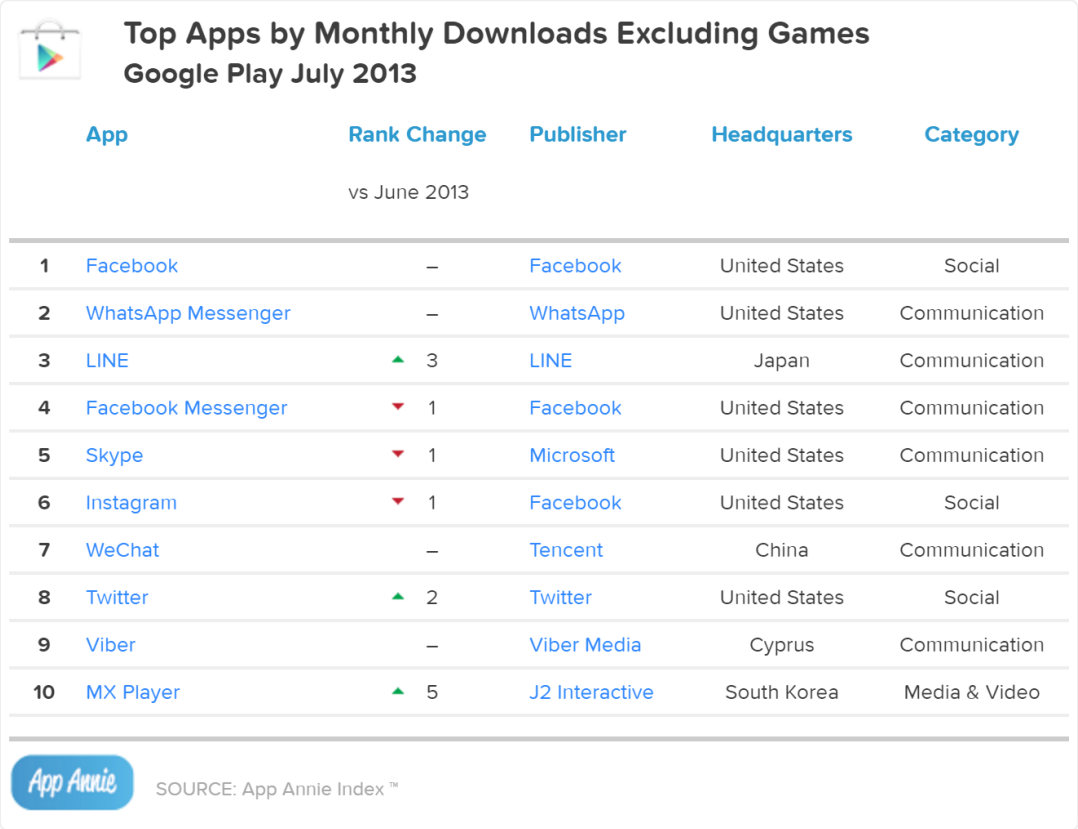
inexpensive implementations with third-party access. EIM implementations include an internal server. For security reasons companies' conversations are encrypted and often archived.

In this study I focused on Consumer IM as applications with broad availability and strong support. The most popular, most secure and other applications which I compare in this project are described below in this chapter.

Android and iOS operating systems hold more than 80% and 13% respectively in the worldwide smartphone OS market share (IDC, 2015). Figure 7 shows Top10 downloaded apps at Google Play and iOS App Store, which are application markets for the Android and iOS operating systems. Six out of ten applications there are instant messengers and three are social networks with instant communication and direct and group messages as well (App Annie, 2013). You may have never even heard of them, but there are millions of people using them around the world. According to recent analytics of App Annie, priority to download IM and communication applications remains high to the present day (App Annie, 2016).

Developers are trying to differentiate themselves, aiming at intact emerging markets and constructing unique experiences that make users feel that they could never live without this particular app, or the friends they have convinced to join. Facebook started as an online social network and is shifting focus on smartphones via Facebook Messenger. Skype, LINE and Viber were originally video conference tools that are trying to develop more nimble and lightweight ways to communicate. Applications let the user play games, send stickers, chat in groups, etc.

The implementation of chat bots extends messengers abilities. For example, it allows translating, searching for video and images, finding by images, converting files or introducing users a new way of receiving information. There are bots in a separate dialog box with commands and an input window, or chatbots which operate right in a group chat. Chat bots are not necessary to add to the contact list. It is enough to mention the bot name on message, and the bot will perform an action.



Top Apps by Monthly Downloads Excluding Games
Google Play July 2013

	App	Rank Change vs June 2013	Publisher	Headquarters	Category
1	Facebook	–	Facebook	United States	Social
2	WhatsApp Messenger	–	WhatsApp	United States	Communication
3	LINE	▲ 3	LINE	Japan	Communication
4	Facebook Messenger	▼ 1	Facebook	United States	Communication
5	Skype	▼ 1	Microsoft	United States	Communication
6	Instagram	▼ 1	Facebook	United States	Social
7	WeChat	–	Tencent	China	Communication
8	Twitter	▲ 2	Twitter	United States	Social
9	Viber	–	Viber Media	Cyprus	Communication
10	MX Player	▲ 5	J2 Interactive	South Korea	Media & Video

App Annie SOURCE: App Annie Index ™

FIGURE 7. Top downloadable apps for the Android OS (App Annie, 2013)

2.3.1 Video conferencing applications

Videotelephony applications provide an exchange of audio-video signals online. Currently LINE and Skype are leaders of web conferencing. Skype, shown in Figure 8, was released in 2003 and was a pioneer of peer-to-peer video communication, allowing web conferencing. Inappropriate usage of bandwidth, mass surveillance and other security concerns are the main reasons to ban Skype in some corporate and government networks. (Tehrani, 2005).

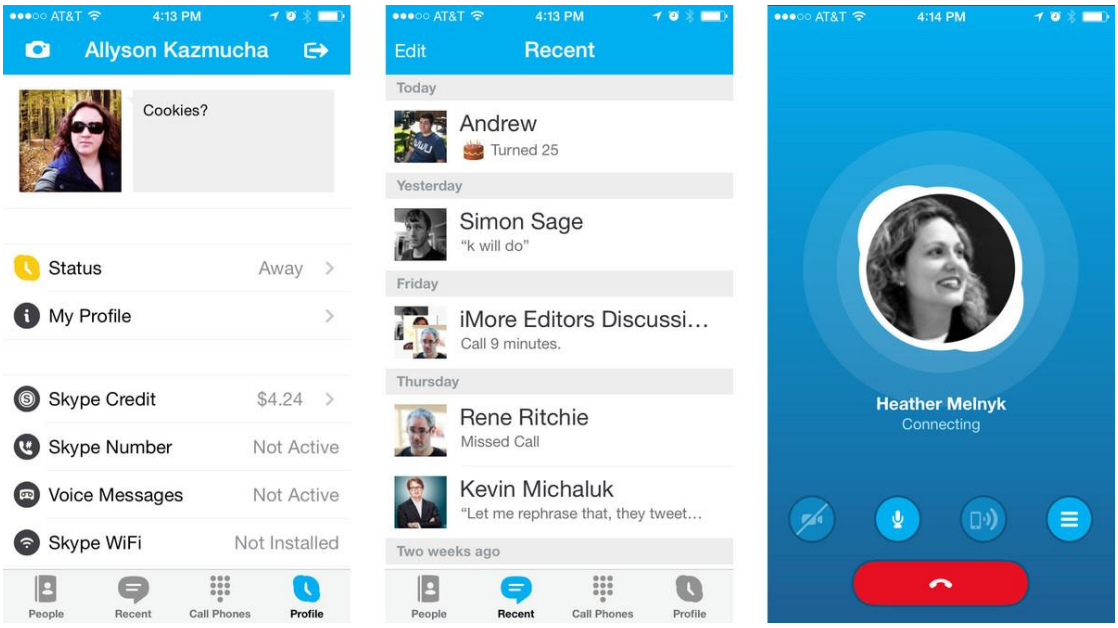


FIGURE 8. Skype mobile app

Tango, Viber, and LINE are concurrent applications and provide the same functionality aiming at mobile devices. The initial releases took place in 2009, 2010 and 2011. The present day LINE, created in Japan, is the leader of mobile video communication and among the top popular IM apps. It has more than 700 million users, features end-to-end encryption and the ability to destroy messages on a specific time (Eun-ji, 2015). The LINE application is shown in Figure 9.

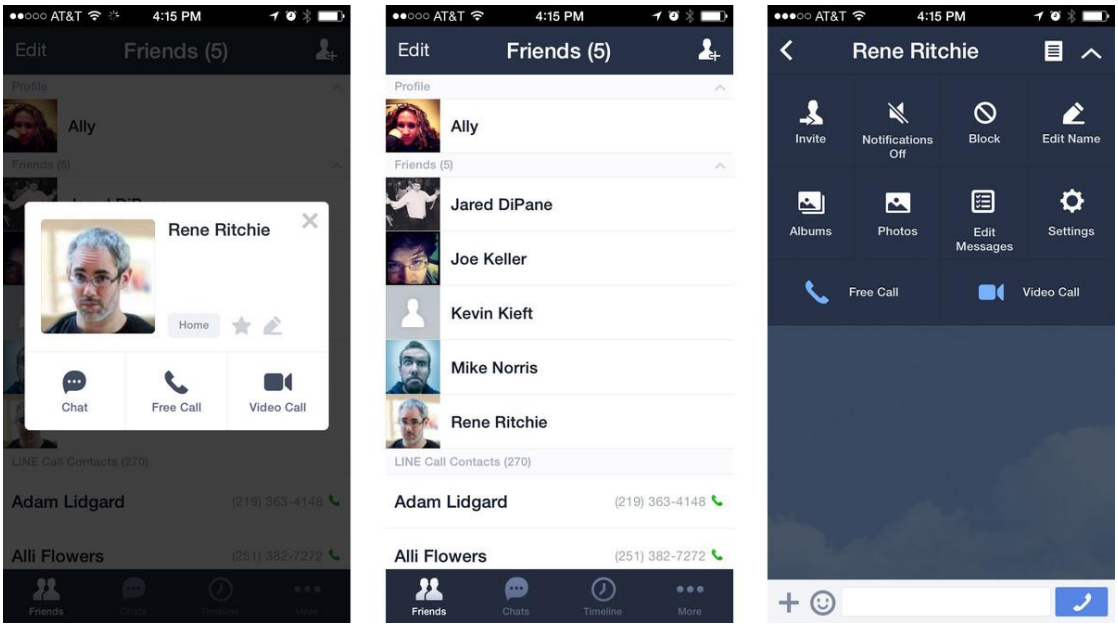


FIGURE 9. LINE

2.3.2 Leading IM applications on Asian market

Asian IM applications dramatically differs from the European and American ones due to culture and politics, e.g. Japan's isolationism and China's censorship. Withal, WeChat, QQ and KakaoTalk lead in the major markets across Asia and are available in worldwide popular languages on a broad number of OS. KakaoTalk is installed on 93% of the smartphones in South Korea (Frier, 2013) under the condition that 88% of the Koreans own a smartphone with Internet access and 94% use the Internet (Poushter, 2016).

WeChat, developed by Tencent, is the largest standalone IM service in China, with over billion users. It provides not only IM features but also payment over the world and city service in China (Tencent Holdings Limited, 2015). Tencent QQ is a variety of services grown from the Open ICQ messenger with currently 853 million active users. The services include IM, games, shopping, music and movies, microblogging and cloud storage (Tencent Holdings Limited, 2016).

2.3.3 Global players' communication software

Corporations like Facebook and Google are among the biggest Internet players. Their messengers concede to single purpose IM apps. However, both Facebook and Google benefits from the number of users who already registered in these companies' products. WhatsApp and Facebook Messenger are on top of the all-time worldwide app downloads (App Annie, 2016). Facebook Messenger integrated with Facebook's chat as a part of disassembling the most famous social network into a set of mobile applications. It has 900 million active users in a month. WhatsApp has a one billion user database, 315 million active daily (WhatsApp Inc., 2016), and acquired by Facebook Inc. on February 19, 2014 (Facebook Inc, 2014). The user interface can be seen in Figures 10 and 11.

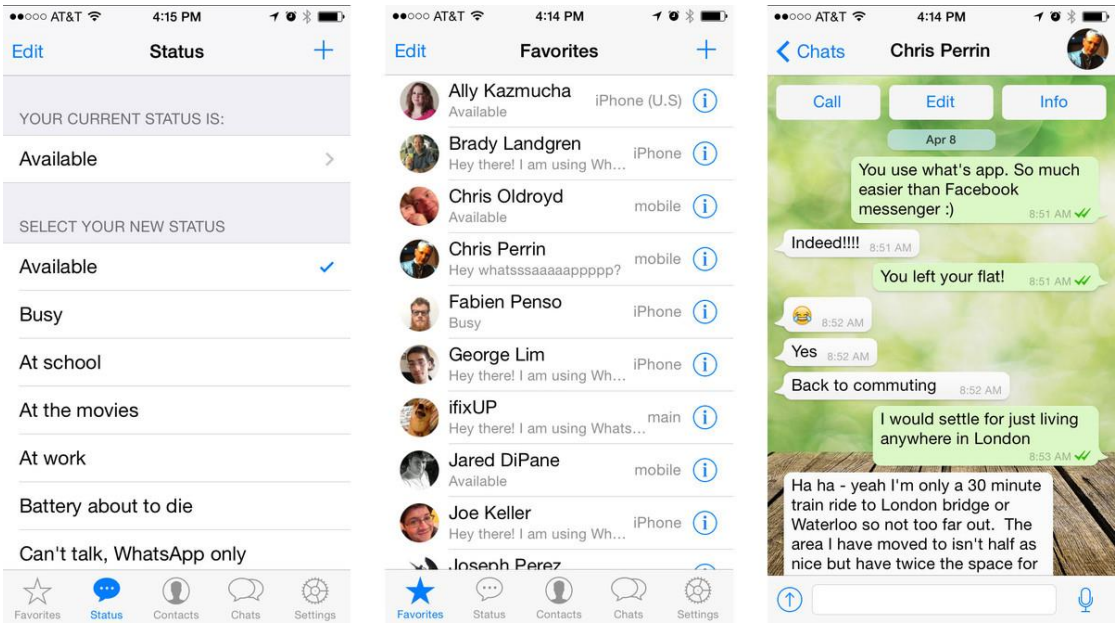


FIGURE 10. WhatsApp

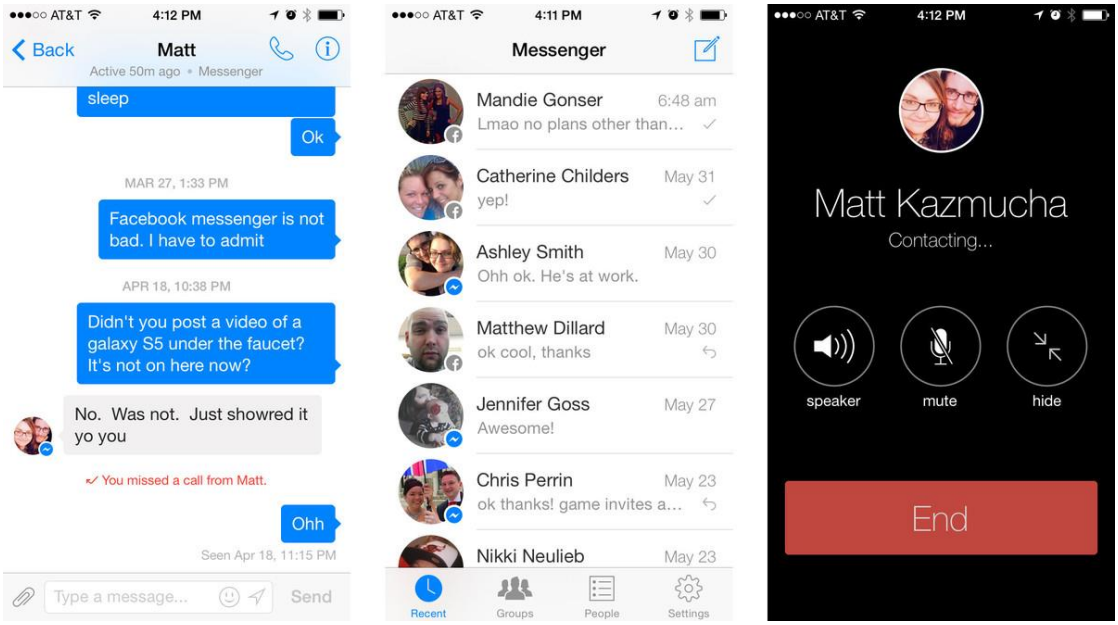


FIGURE 11. Facebook Messenger

Google Hangouts is a communication platform introduced on May 15, 2013. It is currently the default application for text messaging on Android devices. It concurrently replaces previous Google communication services, e.g. Google Talk, Huddle, Google+ video chat (Hamburger, 2013). Hangouts provides IM, VoIP and video conferencing as well as – optional – SMS and voice call to other phones. The app is introduced in Figure 12.

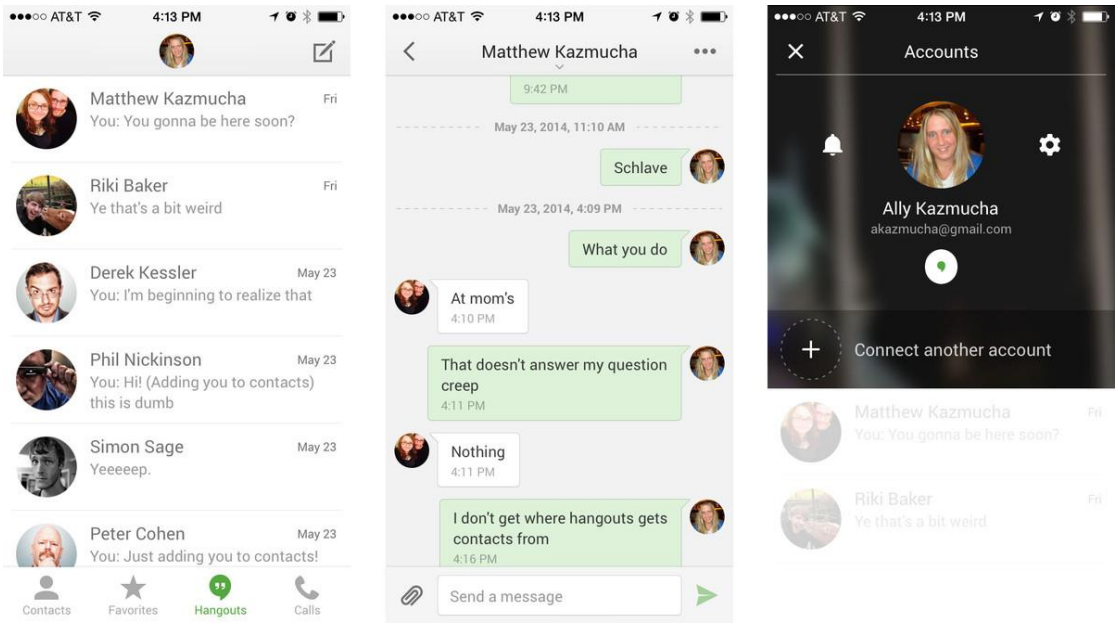


FIGURE 12. Google Hangouts

2.3.4 Secure open-source applications

Open Whisper Systems is a nonprofit open source project with the mission to make private communication simple (Open Whisper Systems, 2016). Organization developed a set of end-to-end encrypted applications: RedPhone and TextSecure for Android and Signal for iOS. Open Whisper Systems merged applications mentioned above into open-source IM software named Signal.

RedPhone is a VoIP encrypted application for Android OS. . TextSecure is a free open source app for SMS and MMS on Android with encryption between application users. These projects discontinued after the merge into one IM app, but applications are still available, and source codes are available under a GPLv3 license (Open Whisper Systems, 2011).

TextSecure provides user-friendly service for end-to-end encrypted IM in private and group chats. However, when the user receives a message from another TextSecure user and has recently entered passphrase in the app, notifications message appear in plain text. While it makes using application easier, it also means that messages are completely visible on smartphone screen without warning. It is an important to set a proper time limit for how long the app can keep passphrase cached because while passphrase cached messenger is insecure.

Edward Snowden is a computer professional who disclosed the National Security Agency and Five Eyes global surveillance and started a dispute about information privacy. He caused increasing awareness in the general public about privacy protection in commodity communication software (Greenwald, MacAskill, & Poitras, 2013). Snowden recommended Signal for iOS, Redphone/TextSecure for Android and posted that he used Signal every day (Beauchamp, 2015). On November 2014, Open Whisper Systems announced a partnership with WhatsApp and that they already incorporated their protocol for Android application (Evans, 2014). On April 5, 2016 WhatsApp announced finishing adding end-to-end encryption protocol in every form of communication on WhatsApp for each OS (Metz, 2016). It is also possible to verify users keys in the app.

Signal is Android and iOS IM software with private chat, encrypted calls, secure file exchange and it works over TOR functionality. There is verification of encryption keys to prevent man-in-the-middle-attack: during the call, the application shows on screen two words from PGP word list – if words match on both ends of the call, the call is secure. On April 7, 2016 Open Whisper System made Signal Desktop publicly available after four months of closed beta testing (Markham, 2016).

2.3.5 The most secure instant messengers

Electronic Frontier Foundation is the international leading nonprofit group founded July 6, 1990 (The Electronic Frontier Foundation, 2015). Organization defending civil rights in the digital world and attracting a lot of attention to user privacy. In this part described IM applications with a high score in the Electronic Frontier Foundation's Secure Messaging Scorecard. Every one of them is end-to-end encrypted and have forward secrecy property, which means the previous communications secure in case the keys are stolen.

ChatSecure has the same characteristics as Signal, but with less user-friendly interface and setup. The application is built on open-source software talk and modified to support the Jabber XMPP protocol (The Guardian Project, 2015). Developed by The Guardian Project - a group that is creating secure open-source applications for communication.

Telegram was created after Edward Snowden relieved NSA snooping. The application provides the ability to communicate in public channels, groups and secret chats, which do not leave a trace on the servers and have self-destruct timer setting. Also it allows

sending different types of files. To reduce delivery time there are servers all over the world.

Silent Circle is paid plan service which consists of two applications: Silent Phone and Silent Text. Silent is an encrypted alternative to Skype, providing IM, voice, video and conference calls. It is possible to communicate in secure way even with a contact who has not installed Silent Text or Phone.

Threema and Wickr are proprietary encrypted IM applications. Threema allows end-to-end encrypted messaging with the ability to verify contacts by scanning private QR code. Wickr created by hacker Nico Sell; application allows setting up self-destruction from few seconds to six days for each message: text, media or file exchange.

iMessage developed by Apple Inc. It is default iOS text messenger with end-to-end encryption. USA government often asks Apple to provide a backdoor access – Apple refuses. The software allows sending text, media, contact information, documents, and group communication.

Cryptocat is a very simple lightweight app which secures text messages. It provides user opportunity to verify independently correspondent's identities. Currently suspended beta, software provide text messaging and file sharing. The initial release was on May 19, 2011.

3 CHALLENGES IN MESSAGING: SECURITY

Concurrently with the development of communication was going evolution of cybercrime. Michelangelo virus appeared in 1992 and considered first destructive virus. In 1995 appeared Macro virus – first to spread through Word documents. In 1999 occurred Happy99, harmless worm hail new year celebration, the first virus to spread through e-mail. The first virus made to profit from infected hosts was Fizzer; it appeared in 2003 (Grimes, 2001).

There is no perfect way to secure any system. It is always a trade-off, unstoppable process, not one-off act. What is secure today may not be secure tomorrow. It is crucially important to continually re-evaluate implemented security practices.

It is also important to understand which information a user protects from whom. Communication can be secured with a strong end to end encryption. Data can be stored on local storage without network access. Metadata is practically impossible to hide. It is data about data - everything about a piece of information, apart from the information itself. Not the content of a message, but information who, to whom, when and where sent it. Legal systems often protect content more than metadata. For instance, in the United States, law enforcement needs the warrant to listen to a person's telephone calls, but claims the right to obtain the list of whom person have called far more easily (Electronic Frontier Foundation, 2014).

According to NowSecure Mobile Security Report, a quarter of mobile applications include one or more high-risk security flaw. 35 percent of communications sent by mobile devices are unencrypted. 43 percent of users do not have a PIN, pattern lock, or passcode. 50 percent of devices connect to the unsecured wireless network at least once a month in the US. Half of the popular applications sent to advertising companies information such as phone number, device ID, information about the calls and the geographical coordinates of the user. (NowSecure, 2016)

Pavel Durov is a supporter of Internet safety concept and a founder of IM application with E2E encryption named Telegram. He affirms that Internet corporates like Google and Facebook effectively hijacked the privacy discourse convincing public that the most important things about privacy are hiding user's public posts, pictures, other data from other users (Telegram, 2015). Adding appropriate settings allow companies to calm down the public attentiveness while given private data to marketers and other third parties (Wired, 2016). Julian Assange as well supports Internet safety concept and he is editor-in-chief of the WikiLeaks, which publishes secret information and classified media. In his book When Google Met WikiLeaks he shares a similar viewpoint, noting that Google - the US company and works closely with the political and military structures, not advertising it to the public (Assange, 2014). Thus, in the modern world, the preference is frequently given to the open source project. Internet privacy should

include protection of private data from eavesdropping third parties like marketers and advertisers, or politics and military.

The necessity for instant messenger is, therefore, to prevent third parties access to the communication between users. At the same time, it is important to control that the service provider does not collect sensitive data and information about the individuals who use these messengers. Different aspect underlies in control how many personal data can be gathered from contact lists and conditions to be added as a new friend. It is vital to stop attempts of using the social network for reconnaissance attacks.

Secure IM specializes in encryption of the message contents providing the key to decrypted information only to the actual users who has access. The idea behind user-friendly secure messenger is to bring secure to the masses, who understand nothing about security. Thus, the application should be not only secure but also fast, powerful and user-friendly.

When used in workplaces an IM application has many useful features, but it also has security risks and liabilities other than described above. There are safety and agreement risks, inappropriate usage and leaking of intellectual property.

3.1 Vulnerabilities and risks

IM session over a using public network allows anybody in the Internet access data transmission. Therefore, strong encryption is crucial. Information transmitted via instant messaging should not be monitored or logged to contribute improved corporate security. Smartphones collect an expanding amount of sensitive data, and it is important to save slight edge between protection of user privacy and protecting company intellectual property.

There are three primary targets for the attacker: data, identity, and availability. Data means sensitive information whenever about a person or company intellectual property. It comes in ways of plain text, authentication login and password, private information or activity logs collected by software.

Stealing identity, usurp it and thus impersonate owner of smartphone grants pass into a bank account or corporation network. Achieved because smartphones very customizable and collect a lot of information about the holderStolen medical identity cost dozen times more than social security or credit card ID (D'Alfonso, 2015).

Availability is understood as reducing the utility or limiting access by the attack to deprive data from the device. It is possible to discharge the battery by launching continuously running application or make smartphone unusable by deleting boot scripts.

Vulnerabilities related to smartphones come from communication like SMS and MMS, Bluetooth, Wi-Fi, and GSM. Other type exploits software vulnerabilities in OS or, for example, web browser. Additionally, there is malicious software that uses weak technical knowledge of users. Furthermore, device theft and loss is an important issue regarding the protection of user privacy. Thus, it is important whether control over the physical device allows access to the message data and if the messages are stored in a secure way on the device itself. Below I will describe how these vulnerabilities can be used and how to protect against them.

3.1.1 Communication-based attacks

SMS attacks are almost no longer relevant for modern smartphones. However, SMS infrastructure is unstable and sending SMS from the Internet causes DDoS attack against telecommunication, which leads to denial of SMS and MMS services.
MMS contain attachments, which may be infected with malicious software, e.g., virus, self-replicated attack over contact list.

The GSM encryption algorithms are from the A5 family. If the network does not support any A5 algorithm implemented by the phone, then the base station can specify the null algorithm A5/0, through which unencrypted radio traffic is sent. Through device capable use 3G or 4G network with strong encryption, the base station can downgrade the radio communication to 2G GSM and specify A5/0 - no encryption (Jøsang, Miralabé, & Dallot, 2015). This is the base for snoop attacks on mobile radio networks using a false base station - IMSI catcher. After breaking GSM encryption algorithm attacker is able to catch all unencrypted communication on a smartphone.

Wireless network connection includes such threats as rogue access points, ad hoc networks, and mutual authentication schemes like WPA2 Group Temporal Key (shared key among all users of the same BSSID). Neglectful users can connect to networks with WEP or WPA (TKIP) outdated security protocols which are quick and easy to hack. Wireless IPS mostly works poorly for mobile devices.

A significant number of devices have Bluetooth turned on all time for pair connection with trendy wearable gadgets. Nevertheless, this standard is exposed to DoS, snoop, and MiTM attacks, resource misappropriation and message modification (Becker, 2007). Steam cipher attacks retrieve encryption key during the day.

3.1.2 Software vulnerabilities: Malicious software

Malicious software are programs that are designed to conduct on a computer actions unwanted by owner. It can secretly record and send data to the third party, steal passwords, change or delete information. Malware usually aims to damage the system and exploits bugs in other programs. It is implemented in three steps: infection, succeed its goal and spread further. Among malware there are Trojans, worms, viruses, etc.

Phishing is a common way to infect the host with malware. It is an innocent looking message with a link or an attachment containing malware. A Trojan is a program allows outside users direct connection. After activation, that always requires user interaction, it infects and deactivates other software and synchronizes with applications to gather data before sending it to a remote server. A worm endlessly self-replicates on multiple hosts across a network. A virus designed to spread to other hosts by embedding itself into legitimate programs and running programs in parallel.

Spyware poses a threat by collecting and spreading a sensitive information without the owner permission or knowledge. Keylogger records everything user type into the device, including passwords and personal information. It might be a software or a physical hardware secretly plugged into the device.

Ransomware blocks user on device and claim payment to unlock the device. The danger to business, especially that depend on immediate access and availability of their information. The probability of a traveling business person pay back to return control under

device is significantly higher because they are at a detriment given bother such as timeliness and unlikely direct access to IT specialists.

Theoretically, OS files on a smartphone are stored in ROM, not hard drives like on the desktop, so malware cannot change it. However, for example, in Windows OS attainable to point on editable file instead of general configurations. Symbian OS is also vulnerable in operating systems settings.

Ghost Push is a program, which automatically gains root access on infected OS, loads malware, changes to system application and at the end revokes root access. Basically, it is impossible to take the infection off by factory reset except when the new firmware is released.

At the present time, numerous antivirus software companies adapt programs to the mobile operating systems, e.g., Avast, Kaspersky Lab, Softwin, Trend Micro. Application distribution systems Google Play and Apple's App Store filter software before publishing to public.

3.1.3 Hardware vulnerabilities: Physical access

Juice jacking is a malware attack utilizing the dual role of USB port as charger and data transmission. Information secretly copied from the device or contrariwise malicious software installed on it over charging port. The threat might be on hard drive with micro-USB connector or concealed in charge adapters.

Smudge attack is a method to recognize and understand graphical password pattern of touchscreen device (Aviv et al., 2010). User's fingers left oily smudges on a glass easily detected under proper lighting; smudge trail remains profitable even after several minutes after unlock and usage. Whisper System reacted with lock screen software resolving the risk (Whisper Systems, 2012).

Jailbroken gadgets simplify for a possible assaulter to gain so-called root access - full administrative control over the machine. A user with root have rights to bypass built-in OS security features, access restricted areas like internal storage, read process memory, install custom firmware, and control kernel.

Against person with a root access any efforts to overcome the threats become useless. No matter encryption, software cannot be called secure under such circumstances. In some countries, for example, United States, rooting is illegal (Electronic Frontier Foundation, 2013). Rooting performed on Unix-like OS including Android to overcome limitations on devices. Jailbreaking is a bypass of Apple restriction for the user on the iOS operating system.

Jailbreaking and rooting have meaning for users' capability to use their devices securely. It might be an essential step preparing installation of security updates after manufacture stopped support for phones or tablets. Another reason, it helps users install convenience software that grants them usage of the device despite disabilities. This is part of the reasons custom firmware become popular.

February 16, 2016, the US Court ordered the FBI to help Apple crack the terrorists' iPhone (Lichtblau & Benner, 2016). Because there is a technical limitation in iOS on the number of wrong password inputs, after which all data is deleted from the device. There is no way, except for password input, to access the data on a smartphone if data was not synchronized with iCloud. CEO Tim Cook has publicly refused to implement a court decision (Cook, 2016).

The rejection from backdoor implementation in iOS is the key principle of the Apple. This shows that iOS 8 and 9 encryption does not allow to hack iPhones after simple password enables and no third party access data if cloud synchronization disabled. However, a group of hackers successfully implement FBI request. Their solution works only for iPhone 5C running the iOS 9 operating system. FBI cannot disclose hacking method because bureau does not have such information itself (Nakashima, 2016)

3.2 Anti-harm solution

The first layer of security lays in operating systems. There is sandbox idea which ensures facilities are safe for themselves, for other apps and data on the system, and the user. Whenever a malware accomplishes to reach a device, it is essential that the OS represents the area that is open to attack as tiny as possible. There are rootkit detectors, file and memory permission, process isolation mechanism helping in case of malware.

Next is software layer. After application installation, first-time requested function ask for authorization to access needed data like contact list, stored media, camera, Internet connection. The user may allow or deny request determining the boundaries of permissible access. These access rules are possible to change or to cancel. On a smartphone rules are located in the device settings, in other cases they are in application settings. Precise control of granted permissions is a part of user awareness.

Smartphones web browsers are vulnerable to phishing, malicious websites, MiTM attacks, etc.; especially rooted devices. This vulnerability can be minimized by keeping software updated and installing anti-virus software.

To avoid phishing attack it is important to be attentive. The user should always check shortened URL and where the link points, verify senders' identity, preferably to use cloud service for file sharing.

Out-of-band verification helps to establish secure communication. It means any way of communication outside of used method. For example, checking public keys in the real world before online communication starts. Secure IM provides the possibility to do it easily with QR codes.

If access to a secret key is lost, there is revocation certificate. In case the key is exposed, revocation certificate announces that user no longer trusts it. Certificate generated in advance, while the user has the secret key, and kept for any future disaster.

The user should use PIN, pattern or password for a device protection. At the same time, use a different password for login into systems, applications or websites. Use two-factor authentication, if it is possible, or install additional software providing such feature. The user should never use the unprotected wireless connection. It is preferable to logout from the application after using it.

4 COMPANY CASE

The main aim of the case is to find a messaging system for a company whose name will not be disclosed due to security reasons. The main purpose is to find a user-friendly

cross-platform application for secure communication in the local network and through the Internet. The chosen app with a new security policy gradually introduces and implements better data protection for the company. The first step is to elucidate the importance of data protection in everyday life and information encryption in business. Simultaneously user-friendly communication software makes employees accustomed with encrypted communication concept.

There are 200 persons working for the company, of which 60 are support staff: food service employees, cleaners, repairers. Company employees spend on business trips from one day to several months. Employees range in age from 23 to 70 years. The level of use and understanding of the technology among various groups varies considerably. The company previously implemented LAN with SAN and iSCSI. This setup provides a file sharing feature for everybody with access to local network. For communication employees use emails and mobile calls.

4.1 Data collection

To find the most suitable solution for the company required information was collected through a survey. The survey contained 15 questions about workers' use of desktop and mobile platforms, the preferable way to communicate and instant messaging experiences, along with knowledge of why communication security is important. The questionnaire is attached in Appendix 1. The participants acknowledged that collected data would be confidential, they could not be personally identified in any analysis or reports, and they are free to withdraw from participation at any time. 127 respondents out of the 140 employees were able to answer, 97 of them answer for each question.

4.2 Survey results

65% of respondents answered they do not travel on business trips while almost 22% spend up to 15 days in a year in business trips. 9% have short trips few days every month and 4% spend time on a long business or educational trips in geographically remote places few months in a year.

As results show in Figure 13, most comfort way of communication are calls (74% respondents choose this answer) and text messages (66%). Less popular are file share

option (45%) and video communication (40%); significantly behind is group communication (26%). At the same time, for work communication text messages appeared more popular – 79% choose this answer. Calls also gain a little bit more power (80%). There is almost no difference in the video calls rates – it increased less than one percent. Group communication and sending files are indicated as frequently used, their evaluations increase more than 20%.

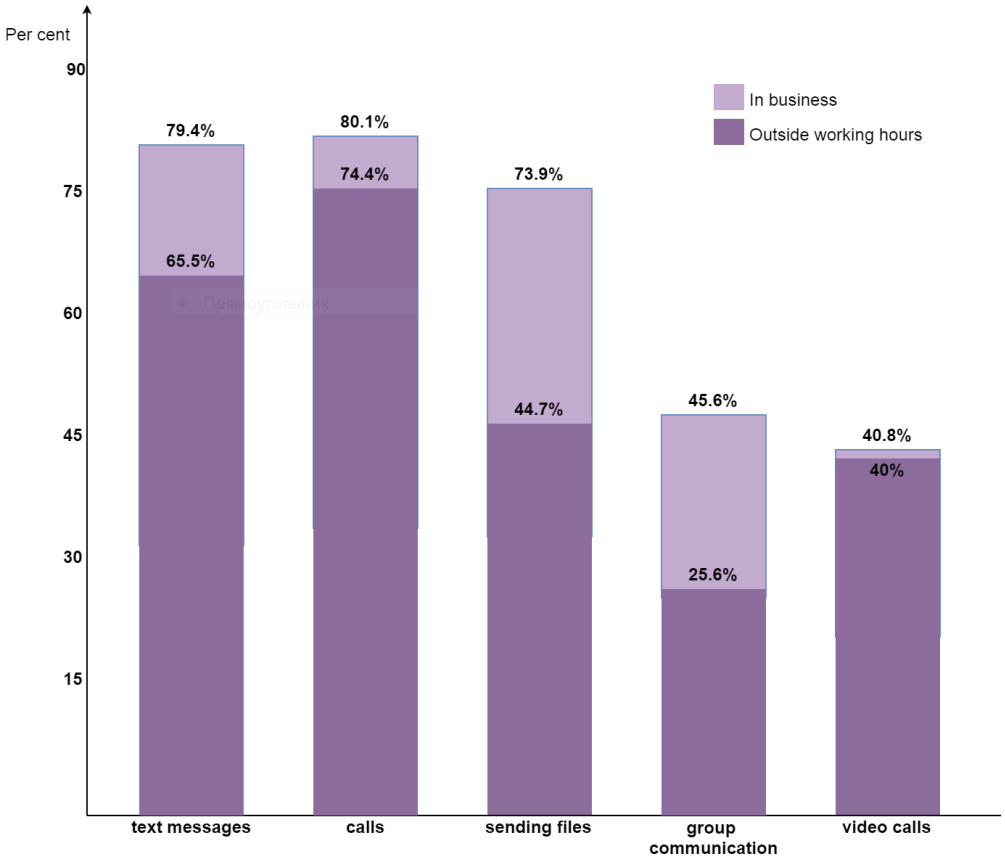


FIGURE 13. Popularity of communication types

The survey discovered that 3% of respondents use messengers occasionally. They use IM only because of work need, not by their own wish. More than 60% use messengers every day, 5% every week and nearly 30% from time to time. Two persons pointed that they try to reduce usage of smartphone and use IM only during trips.

The second part of survey conduct questions about OS and applications respondents know already. 67% use some Android smartphone, 12% use iOS devices, and 14% prefer to use a simple cell phone. 3% use Windows Phone or older Nokia. 4% found

difficult to answer which OS was installed on their devices. The system administrator helped to gain missing information.

Absolutely everybody including system administrators uses Windows OS on their desktop computers. Even when working remotely, employees choose Windows OS in their PC or laptop. Somewhat it partly necessity for laboratory personnel, because they use specific software appropriate only for Microsoft products. The Company has no policy obliging installation a particular OS on the working PC apart from for laboratory staff.

70% of responders have used messengers' systems for more than five years, 20% - from two to five years, 5% use one to two years or less than a year. Most popular way of communication is messages in social network VK, broadly popular among Russian-speaking users. However, the Company chooses to leave this service for personal life and also block access to the social network from the corporate LAN by firewalling.

More than 50% of employees already use Skype, Mail.ru Agent, or Viber. Skype and Viber are popular due to web conferencing feature, which allows video communication at long distances, which has a reason in a vast country. Mail.ru Group attracts users by domain name and Mail.ru Agent connects a phone number, corresponding e-mail and most popular in Russia social networks together.

40% use WhatsApp, 26% do not use any social instant messenger (except for business) but e-mail, 13% use Facebook Messenger and 11% Google Hangouts, 8% use Telegram. Other applications do not reach 7%, so they are not included.

Determining willingness to start using the new application, 38% evaluate it as 4 points out of 5, 23% are located to either side of this evaluation. 14% have not expressed the desire to learn new at all, 2% agree but without aspiration.

Last part of the survey gathered information about knowledge and understanding the importance of security on the Internet. 82% of respondents answered that it is critical to have the protected connection. 18% choose a rating of 4 points on a scale of 5 where are five stands for crucial. However, as can be seen in Figure 14, the importance of secure connection and encryption for communication in the business area obtained allocation along the entire scale.

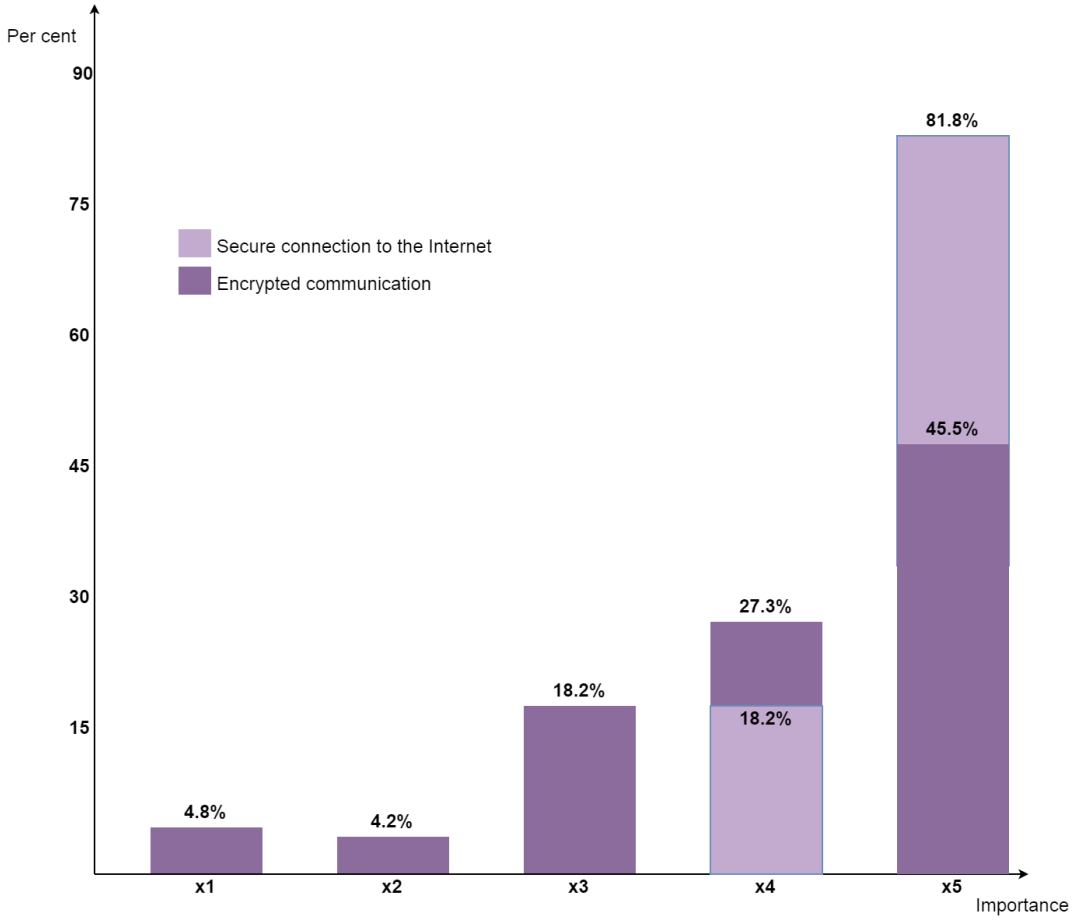


FIGURE 14. Secure or encrypted connection importance

5 APPLICATION SELECTION

The collected information helps to choose appropriate software and substantiate the choice. The case company requirements include high availability, end-to-end encryption, user-friendly interface, file sharing and group communication. Regarding security, additional circumstances require authentication, authorization, and access control. Management requires the possibility to administer safety and to supervise groups. The selection of social network communication is forbidden.

Business and educational trips often happen in places where it is difficult to make calls: noisy places with a poor connection. Therefore, from the company point of view calls over applications are less important than text messages and the possibility to share different types of files.

5.1 Data analysis

35% of employees travel on business trips or participate in education trips within a year. The preferable ways of communication are calls, text messages and sending files. Group communication is important in business communication to approximately half of the respondents. Video calls are used by 15% of employees.

As mentioned earlier, 4% of employees do not know which OS was installed on their devices. It is important to mention that fact to assess the level of technical knowledge. The company employees are people of 20 to 70 years old. Many elderly people do not bother about devices. They prefer to rely on and trust the decision on the device choice made by their close ones who better understand new technology.

In general, employees agreed to start using the new IM application. Everybody had already use e-mails and text instant messengers. More than half use video conferencing software and 40% use WhatsApp. It can be conducted that there are no problems with IM use. Windows is completely dominant as a desktop operating system. Yet, other OS should not be ignored as the company has no policy obligating the installation of a particular OS on the work PC. Among mobile OS employees use there are Android, iOS, Symbian and Windows Phone.

Participants found a secure Internet connection is necessary. This probably leads to less attention to encrypted communication. It is a widespread misconception that a protected connection already provides secure communication. There is a need to expose and enhance the knowledge why it is important to encrypt data even with a secure connection.

I wrote a series of short posts about the importance of an end to end encryption. It is fast to read, easy to understand and has simple everyday examples. In addition, a short presentation with Q&A series was conducted afterward when the chosen IM application was introduced to employees. It was aimed especially at the employees who preferred not to spend time on reading posts. Such presentation gives an answer why the company wanted to use IM software for internal communication.

5.2 Application filtration

I collected information about 25 messaging applications. The full comparison table is attached in Appendix 2. The analysis proceeded based on the CIA triad and additional authentication criteria. The first parameter for sorting is the type of instant messaging and features: text, voice and video calls, group communication, secret chats and types of file transmission. The next parameter is the protocol the application is based on. The next three parameters are CIA: Confidentiality implies encryption, Integrity means message verification option, and Availability embodies operating systems, language, license, and cost. The last parameter is authentication that comprises the user and author verification.

The first stage of selection checks availability: e.g. Threema is available on few mobile OS, but not on the desktop or the web. Thus, this application is unsuitable. Moreover, IM allows groups up to 50 users maximum. Some applications did not pass the selection stage based on the implemented encryption method. For example, Skype does not encrypt part of the call over PSTN. The problem is that popular applications do not implement end-to-end encryption and forward secrecy, and secure applications are not widely available.

After using certain selection criteria several IM remained for testing. They are Signal, Telegram, WhatsApp and LINE. Signal is an open source secure messenger providing the necessary features. LINE as a proprietary application with great VoIP and video communication solution. Telegram is an open source secure messaging app with the ability to send any types of files. WhatsApp provides text and voice communication and announced in April 2016 to support end-to-end encryption on every device.

Originally considered Threema and Wickr did not take part in the final selection for the following reasons. Positively, Threema has the possibility to communicate from the company name with non-registered users, sends any type of files up to 20 MB, and has simple, user-friendly verifications using three dots. Notwithstanding, Threema costs at least USD 2 per license, works only on smartphones as has no web version, allows groups up to 50 users only, and does not have instant calls and video. Wickr has a desktop and mobile versions. It is free and developing business features. Wickr groups up to 10 persons only and has no instant calls and video features.

All applications reaching the final round can be considered to be free and to have strong encryption. Messengers need a mobile phone number for registration and might be used at several devices at the same time. Signal and WhatsApp have the option for users' independent key verification.

As can be seen in Table 1, all tested applications provide instant text messengers and a convenient group size. It is necessary to add that multimedia messages in WhatsApp are sent to an HTTP server first. Telegram is the only application allowing sending any file up to 1.5 GB in size each. There also two kinds of groups: up to 200 users and supergroups of up to 5 000 with option to disable stickers to avoid overloading the communication. LINE provides bulletin boards in chat on which users can add posts, likes and comments.

The tables below use color coding. Green means that the value is fulfilling the case company requirements, red – not satisfying, yellow – in-between, negotiable. This is a simplified version of the full table for the comparison of instant messengers available in Appendix 2.

TABLE 1. Type of instant messaging

	text	voice	video	group chats	files adding
Signal	yes	yes	no	yes	image, video, audio, contact, location
LINE	yes	yes	yes	up to 200 users	image, audio, videos, current or any specific location
Telegram	yes	no	no	up to 200 or 5000 users	image, audio, video, files of any type (doc, zip, mp3, etc)
WhatsApp	yes	yes	no	up to 256 users	pdf, image, audio, video

Table 2 comprises a software availability comparison. Every IM app is accessible from Android, iOS and the web. However, LINE has no website option, only the Chrome browser app. That fact might set some limitations. Telegram has both the web and Windows desktop clients. Signal has the poorest choices: it is not available on less popular mobile OS. However, all employees with Windows Phone or Symbian OS smartphones either have another Android device or do not travel on business purpose.

TABLE 2. Availability

	Mobile				Desktop		
	Android	iOS	WP	Others	Web	Windows	Other
Signal	yes	yes	no	no	yes		
LINE	yes	yes	yes	BlackBerry, Nokia Asha series	Chrome App	yes	Mac OS X Firefox OS, ChromeOS
Telegram	yes	yes	yes	Ubuntu Touch, Firefox OS	yes	yes	OSX, Linux, and UNIX-like
WhatsApp	yes	yes	yes	Nokia S60, Nokia S40 EVO, BlackBerry and BlackBerry 10	yes		

LINE has a lot of additional features, and some may disturb business processes, e.g. games and tv, and some may help in some cases, e.g. dictionaries, additional accounts, lightweight app version. Signal sometimes has problems with the phone number verification through SMS. In this case, a user needs to call and listen to six numerals in English and then input them manually. An additional aspect of security can be found in Telegram bots. An antivirus software company added a chat bot in the application, which can scan files and links for threats. In case there is a risk, the bot will send a malware name and link to the description in the virus database. Chatbot can be used in group communication.

5.3 Testing

There were formed three groups from 22 volunteers. Groups' members equally diverse based on the indications of technical knowledge, age, smartphone skills and software user experience. Starting on 28 March these teams were testing Signal, Telegram, LINE and from 7 April WhatsApp. Table 3 contains a brief summary of the testing results. Media stands for images, video and audio from the host memory.

TABLE 3. Application comparison

	Registration and phone number verification	Key verification	Instant communication	Files	Notification about logging in other device	Privacy	Problems
Signal	SMS or listen for code	key or QR code, two words during the call	text, calls	media, contact, location	no, but shows active sessions	passcode lock, do not allow screenshots	notifications errors, contact sharing, unread messages shown from last one
Signal Web	scan QR code a with smartphone	key	text	media	no		desktop application does not load previous conversation from other devices
LINE	SMS	no	text, calls, video	media, location	yes		application opens several seconds
LINE Web	scan QR code with a smartphone	no	text	any type of files	yes, logs out if the user use another PC	logout when the user closes the app	unread messages shown from last one, log out when the user closes the
Telegram	SMS	no	text	any type of files	yes, also shows active sessions	passcode lock, two-step verification	no message forwarding into secret chats, no group secret chats
Telegram Web	SMS or code in application	no	text	any type of files	yes, also shows active sessions	set additional password	secret chats are not shown
Telegram PC	code in the application	no	text	any type of files, recorded audio	yes, also shows active sessions	local passcode, two-step verification	secret chats do not shown
WhatsApp	SMS	key or QR code	text, call	media, contact, location, document	no, but shows active sessions		all documents transformed into a pdf file
WhatsApp Web	SMS	no	text	media, recorded audio and camera photo	no		documents and contacts do not download or do not viewed fully, just preview

Signal smartphone application has problems with receiving SMS code. In some cases, if the application was not open, Signal does not notify the user about calls and mark them as missed. Contacts send as just one phone number without name or possibility to send all contact information like few mobile numbers at once. To view a video a user should agree with the app warning that data will be decrypted and written to the device storage. For easier identity verification a user should install an additional application – barcode scanner – to display or scan QR code. At the same time, there are still option to check numeric codes. During a call a user can independently verify the identity of the caller by comparing key fingerprints out-of-band with simply two words appearing on screen. Signal does not allow screenshots when the application is open.

Signal desktop app does not load a previous conversation from a smartphone. Media attachments – image, video, audio, map – are loaded immediately. It is possible to attach audio, video and images in the desktop version. The app is an extension for the Google Chrome browser that works in a separate window. New messages read all at once, showing from the last one, not from the first unread one.

WhatsApp always loads previous conversations. Media files are loaded immediately.In a desktop version a message with contacts information does not appear properly and includes only a name and image. On the smartphone version it is possible to view shared contact details, e.g. e-mail addresses and mobile numbers, and to invite or add a contact into the contact list.

LINE allows sharing only the contacts the user has in the application, not on a smartphone. Also, the application gives the possibility to send any type of attachments in the desktop version. It is easy to receive and open them on a smartphone. The desktop app is an extension for the Google Chrome browser, which works in a separate window. Desktop LINE log out when a user closes the application window or login from another desktop. Automatic logout from the web application can be used to provide remote security.

Telegram allows secret chats only on smartphones. Such chats are not supported on the desktop version. Telegram has two options for PC users: a web-browser solution and desktop software. They are quite similar.

5.4 Results

After the testing there was a voting to choose the application. The poll considered votes of employees from testing groups, Chief Technology Officer, Chief Executive Officer, Chief Operating Officer, Director, Manager Director, Senior vice-president and IT system administrator. These 30 persons have given scores for messengers' various security and usability features.

The weighted score is calculated based on testing results as shown in Table 4. First two columns contain the criteria and their weight. The following criteria were used: instant communication, privacy, key verification, user friendliness, files sending, notification about logging in another device, registration and phone number verification. Instant communication criterion stands for types of real-time information exchange. Privacy includes additional security steps, for example, password protection and two-step verification. Key verification means the possibility to check encryption keys to avoid MiTM attack. User friendliness is a subjective criterion which assesses the interface usability when the application used continuously and when the user for the first time gets acquainted with the system. Files sending means types of files, media and other information it is possible to send and receive on mobile and desktop applications. Notifications about logging in another device is a secure feature which alerts about hacking. It also includes if the application shows active sessions and gives the possibility to terminate them. Registration and phone number verification usually happens once, thus, they counted together. Additional criterion assessed the problems that have been identified during testing.

Each application can gain from 1 to 4 points for each criterion, and the greater number is better. In case of applications conform the criteria equally, each of these apps gets the arithmetic mean of the closest points. The last row in the table contains the sum of points multiplied by the corresponding criterion weight. As a result, each application can gain from 0.9 to 8.1 points. So, for example, LINE has best communication options, because it provides text, calls, and video communication. Thus, the application gets 4 points for the first criterion with weight 0.4. Total amount of points is equal to $4 \cdot 0.4 + 2 \cdot 0.4 + 1 \cdot 0.3 + 1 \cdot 0.3 + 3 \cdot 0.3 + 3 \cdot 0.2 + 1 \cdot 0.2 - 1 \cdot 0.3 = 3.5$.

TABLE 4. Evaluation

Criteria	Weight	Signal	LINE	Telegram	WhatsApp
Instant communication	0.4	2.5	4	1	2.5
Privacy	0.4	3	2	4	1
Key verification	0.3	4	1	2	3
User friendliness	0.3	2	1	3	4
Files sending	0.3	1	3	4	2
Notification about logging in other device	0.2	1.5	3	4	1.5
Registration and phone number verification	0.2	2	1	4	3
Problems	-0.3	3	1	4	2
Sum		4.1	3.5	5.1	4.4

Signal succeed in key proof because application provides simple two-word verification during the call. Application considered as a secure one, so it attains good outcome in privacy as well, but it is not user-friendly. Software lost a lot of points because of problems testing group found earlier. As mentioned before, LINE has the best communication options. It also succeeds in files sending and logging notifications. Since LINE is not considered as a secure application, privacy and other security criteria evaluated low. Also, LINE has overloaded by additional functions interface.

WhatsApp evaluated as most user-friendly. It has a simple and clean interface with three windows: calls, messages and contact list. IM attained good outcome in key verification, registration, phone number verification, and instant communication criteria. Telegram aims to bring security to the masses. The application manages to balance user friendliness while remaining protected. This IM got the highest grade in logging notification, registration and phone number verification, file sending and privacy criteria. At the same time, problem criterion gained the highest rate also. According to evaluation table, best application is Telegram. However, high security available only in secret chats, which, from the other point of view, concedes in usability.

Reverting to the survey results in chapters 4.2 and 5.1, it is important to take in the account two more criteria in application selection. Firstly, the fact that level of use and understanding of technology among the Company employee various considerably.

Secondly, currently used IM and willingness to start to use the new application. Examinating together survey results and tables output, voting group choose WhatsApp application. Among the advantages of WhatsApp is the fact that 40% of employees answer in the survey that they use it already. Application provides an opportunity to create groups up to 256 users and send files and media. It was decided to use WhatsApp application currently and keep an eye open for new developments in IM world. In my opinion, it is a wise solution because WhatsApp implements new features and develops all the time. In case usage of instant messengers justify itself, company management would like to apply a secure paid solution.

6 CONCLUSIONS

Nowadays the Internet and smartphones are a substantial part of everyday life. It helps us to be in touch with others and to manage business projects more easily. Instant messengers entrenched in the online communication world a long time ago. IM immediately adapts to the possibilities of digital sphere and to human requirements. Nowadays, messenger applications try to conquer even greater significance. Instant messengers are gradually replacing other software making it possible to perform a necessary function through IM apps by bots, for example.

The practical aim of the study was to find a free of charge instant messenger with the end-to-end encrypted connection. The desirable result should allow groups up to 200 people, send different types of files and has a desktop version.

The theoretical aim was to review the development of IM and security features, as well as to review current popular and secure mobile messaging applications. I should pay attention that everything changes very fast in Internet communication. It is important to keep eyes open. During the time of writing this project several applications appeared and ceased to exist. Other apps have introduced new features in the form of encryption or have been actively promoting bots and other features. For example, by the end of the experiment, Viber has implemented end-to-end encryption and Facebook Messenger introduced money transaction, file sharing via Dropbox, group video calls up to 50 people and chat bots. It is not possible to secure users, data or devices from every threat.

Metadata is still available in any case. However, it is possible to reduce risk in dozens of times by implementing basic configurations.

Every study has its limitations, and it is important to observe them for further development and to evaluate the whole work competently. My thesis pointed out that in the selection of the software we have to take into account both the software and the context where it will be used. In this study, I analyzed these things separately. However, developing a general model which combine both of these would be a fascinating area of future study.

Further development for the case company involves improving smartphones security including passwords, antiviruses, and monitoring application. For a local network I suggest NAS instead of SAN, because it will be more suitable file sharing service. Use free proprietary software for instant messaging communication is not the best solution. However, it is a first step in becoming accustomed to encryption and basic security measures in business and everyday life. Probably, VPN is also useful.

BIBLIOGRAPHY

Abbruzzese, J. (2014, 4 15). *The Rise and Fall of AIM, the Breakthrough AOL Never Wanted.* Retrieved from Mashable.com: http://mashable.com/2014/04/15/aim-history/#r974Zt0lqgqC

App Annie. (2013, 8 28). *App Annie Index: Apps – Messenger Apps Go To Battle For The World's Messages.* Retrieved from App Annie: http://blog.appannie.com/app-annie-index-apps-july-2013/

App Annie. (2016, 2). *App Annie Index.* Retrieved 4 4, 2016, from App Annie: https://www.appannie.com/indexes/all-stores/rank/overall/

Assange, J. (2014). *When Google Met WikiLeaks.* New York and London: OR Books.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). *Smudge Attacks on Smartphone Touch Screens* . 4th USENIX Workshop on Offensive Technologies.

Beauchamp, Z. (2015, 5 24). *The 9 best moments from Edward Snowden's Reddit Q&A.* Retrieved from Vox Media: https://www.vox.com/2015/5/21/8638251/snowden-reddit

Becker, A. (2007, 8 16). *Bluetooth Security & Hacks.* Ruhr-Universität Bochum.

Cook, T. (2016, 2 16). *A Message to Our Customers.* Retrieved from Apple Inc. : http://www.apple.com/customer-letter/

D'Alfonso, S. (2015, 2 3). *The Growing Problem of Medical Identity Theft.* Retrieved from security intelligence: https://securityintelligence.com/the-growing-problem-of-medical-identity-theft/

Electronic Frontier Foundation. (2013, 1 28). *Is It Illegal To Unlock a Phone?* Retrieved from Electronic Frontier Foundation: https://www.eff.org/is-it-illegal-to-unlock-a-phone

Electronic Frontier Foundation. (2014, 11). *Surveillance Self-Defense* . Retrieved from EFF: https://ssd.eff.org/en/glossary/metadata

Enterprise Storage Group. (2003, may). *ESG compliance report excerpt.* Retrieved from techtarget.com: http://searchstorage.techtarget.com/tip/ESG-compliance-report-excerpt-Part-1-Introduction

Eun-ji, B. (2015, 2 8). *Number of Line users to top 700 mil. this year.* Retrieved from Korea Times: http://www.koreatimes.co.kr/www/news/tech/2015/02/419_173201.html

Evans, B. (2015, 12 18). *16 mobile theses.* Retrieved from ben-evans.com: http://ben-evans.com/benedictevans/2015/12/15/16-mobile-theses

Evans, B. (2015, 3 30). *Messaging and mobile platforms.* Retrieved from ben-evans.com: http://ben-evans.com/benedictevans/2015/3/24/the-state-of-messaging

Evans, B. (2016, 3). *Mobile Is Eating the World (2016).* Retrieved from www.slideshare.net: http://www.slideshare.net/a16z/mobile-is-eating-the-world-2016/6-6And_tablets_add_a_quarterbillion

Evans, J. (2014, 11 18). *WhatsApp Partners With Open Whisper Systems To End-To-End Encrypt Billions Of Messages A Day*. Retrieved from TechCrunch.: http://techcrunch.com/2014/11/18/end-to-end-for-everyone/

Facebook Inc. (2014, 2 19). *Facebook to Acquire WhatsApp.* Retrieved from newsroom.fb.com: http://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/

Frier, S. (2013, 12 23). *With $200 Million in Revenue, South Korea's Top Messaging App Is All Smiley Faces.* Retrieved from Bloomberg:

http://www.bloomberg.com/news/2013-12-22/with-200-million-in-revenue-south-korea-s-top-messaging-app-is-all-smiley-faces.html

Gagné, M. (2003, 3 1). *Chatting Up the Chef.* Retrieved from linux journal: http://www.linuxjournal.com/article/6489

Garling, C. (2011, 12 20). *Twitter Open Sources Its Android Moxie*. Retrieved from wired.com: http://www.wired.com/wiredenterprise/2011/12/twitter-open-sources-its-android-moxie/

Greenwald, G., MacAskill, E., & Poitras, L. (2013, 6 11). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* Retrieved from The Guardian: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Grimes, R. A. (2001). *Malicious Mobile Code: Virus Protection for Windows.* Sebastopol, CA: O'Reilly.

Hamburger, E. (2013, 5 15). *Exclusive: Inside Hangouts, Google's big fix for its messaging mess.* Retrieved from The Verge: http://www.theverge.com/2013/5/15/4318830/inside-hangouts-googles-big-fix-for-its-messaging-mess

Hansell, S. (1998, 6 9). *America Online to Buy Internet Chat Service for $287 Million.* Retrieved from New York Times: http://www.nytimes.com/1998/06/09/business/america-online-to-buy-internet-chat-service-for-287-million.html

Hoyos, B. D. (2008, 3 15). *The World's First IMs.* Retrieved from about tech: http://im.about.com/od/imbasics/a/imhistory_2.htm

IBM Security. (2015, 12 9). *Making Mobile Messaging Manageable and Secure.* Retrieved from youtube.com: https://www.youtube.com/watch?v=8GTJTcqw1tk&A=SM_BLOG_SI_SEM&O=SM

IDC. (2015, 8). *Smartphone OS Market Share, 2015 Q2.* Retrieved from idc.com: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Jøsang, A., Miralabé, L., & Dallot, L. (2015). *It's not a bug, it's a feature: 25 years of mobile network insecurity.* European Conference on Cyber Warfare and Security.

Kessler, S. (2010, 10 11). *Fun and Safe Social Networks for Children.* Retrieved from Mashable: http://mashable.com/2010/10/11/social-networks-children/

Lichtblau, E., & Benner, K. (2016, 2 17). *Apple Fights Order to Unlock San Bernardino Gunman's iPhone.* Retrieved from The New York Times (Washington, D.C.): http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0

Mail.Ru Group. (2015, 11 20). *Как у Аськи лицо менялось: визуальная эволюция интерфейса ICQ.* Retrieved from habrahabr: https://habrahabr.ru/company/mailru/blog/271317/

Markham, L. K. (2016, 4 7). *Signal Desktop beta now publicly available.* Retrieved from whispersystems.org: https://whispersystems.org/blog/signal-desktop-public/

Metz, C. (2016, 4 5). *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People.* Retrieved from Wired: http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

Nakashima, E. (2016, 4 12). *FBI paid professional hackers one-time fee to crack San Bernardino iPhone.* Retrieved from Washington Post: https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

NowSecure. (2016, 2 11). *2016 NowSecure Mobile Security Report.* Retrieved from NowSecure: https://info.nowsecure.com/2016-NowSecure-mobile-security-report_download.html?aliId=2284881

Oikarinen, J. (2010). *Founding IRC.* Retrieved 3 2016, from mirc.com: http://www.mirc.com/jarkko.html

Open Whisper Systems. (2011). *https://github.com/WhisperSystems*. Retrieved from Github: https://github.com/WhisperSystems/Signal-Android

Open Whisper Systems. (2016, 2 13). *Open Whisper Systems.* Retrieved from Open Whisper Systems: https://www.whispersystems.org/

Patel, N. (2014, 1 2). *Global Mobile Messaging Forecast (2001 - 2017).* Retrieved from strategy analytics: https://www.strategyanalytics.com/access-services/media-and-services/mobile/wireless-media/wireless-media/reports/report-detail/global-mobile-messaging-forecast-(2001---2017)#.VuWF3fmLT3Q.

Patel, N. (2015, 6 3). *Global Mobile Messaging Forecast (2001-2021).* Retrieved from strategy analytics: https://www.strategyanalytics.com/access-services/media-and-services/mobile/wireless-media/wireless-media/reports/report-detail/global-mobile-messaging-forecast-(2001-2021)np3#.VuWHVfmLT3Q

Poushter, J. (2016, 2 22). *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies.* Retrieved from Pew Research Center: http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

qlinklives.org. (2007, 6 14). *Screenshot of a Quantum Link OLM.* Retrieved from qlinklives.org: http://www.qlinklives.org/qlink-old/liz1.jpg

riko. (2009, 4 16). *Archive of all versions of ICQ clients.* Retrieved from riko.ws: http://riko.ws/?p=367

Talmesio, D. (2016, 2 9). *One SIM per person on the planet, but still too many unconnected.* Retrieved from Ovum: http://www.ovum.com/press_releases/one-sim-per-person-on-the-planet-but-still-too-many-unconnected/

Tehrani, R. (2005, 11 10). *Ban Skype*. Retrieved 1 10, 2016, from TMCnet: http://blog.tmcnet.com/blog/rich-tehrani/voip/ban-skype.html

Telegram. (2015). *What are your thoughts on internet privacy?* Retrieved from telegram.org: https://telegram.org/faq#q-what-are-your-thoughts-on-internet-privacy

Telegram. (2015). *Hash Collisions for Diffie-Hellman Keys.* Retrieved from Telegram APIs: https://core.telegram.org/articles/DH_Hash_Collision

Tencent Holdings Limited . (2016, 3 17). *Tencent Announces 2015 Fourth Quarter and Annual Results.* Retrieved from Tencent: http://tencent.com/en-us/ir/news/2015.shtml

Tencent Holdings Limited. (2015, 8 12). *Tencent Announces 2015 Second Quarter and Interim Results.* Retrieved from http://tencent.com/: http://tencent.com/en-us/ir/news/2015.shtml

The Electronic Frontier Foundation. (n.d.). *About EFF.* Retrieved 4 1, 2016, from The Electronic Frontier Foundation: https://www.eff.org/about

The Guardian Project. (2015, 7 15). *Secure Mobile Apps.* Retrieved from GuardianProject.info: https://guardianproject.info/apps/

United States Patent and Trademark Office. (2006, 1 16-20). *Summary Of Final Decisions Issued By The Trademark Trial And Appeal Board.* Retrieved from www.uspto.gov: http://www.uspto.gov/web/offices/com/sol/foia/ttab/decsum/2006/16jan06.pdf

Usuario:Porao. (2006, 1 15). *Unix talk screenshot 01.* Retrieved from wikimedia.org: https://commons.wikimedia.org/wiki/File:Unix_talk_screenshot_01.png

WhatsApp . (n.d.). *How do I use WhatsApp Web?* Retrieved from WhatsApp: https://www.whatsapp.com/faq/en/web/28080003

WhatsApp Inc. (2016, 2 1). *One billion - WhatsApp Blog.* Retrieved from WhatsApp: https://blog.whatsapp.com/616/One-billion

Whisper Systems. (2012, 6 28). *Android and data loss protection*. Retrieved from whispersys.com: https://web.archive.org/web/20120628215540/http://www.whispersys.com/screenlock.html

Wired. (2016, 2 23). *Telegram's Pavel Durov: Podcast 256.* Retrieved from wired.co.uk: http://www.wired.co.uk/podcast/episode-256

APPENDICES

6.1 Questionnaire

1. What is your age?

2. How much time do you spend on business trips?
   I do not travel in business trips
   1-10 days in a year
   Few days every month
   2-6 weeks in a year
   I travel in long business trips: 2-8 months in a year
   I work from home

3. Which ways of communication do you prefer to use?
   Text messages
   Calls
   Video conferencing
   Sending files
   Group communication

4. Which ways of communication do you need to use in business communication?
   Text messages
   Calls
   Video conferencing
   Sending files
   Group communication

5. Evaluate the importance of the possibility to communicate by using next types of IM:
   Text messages
   Calls
   Video conferencing
   Sending files
   Group communication

6. How often do you use IM clients?
   Daily
   Weekly
   From time to time
   Only during business trips

7. What mobile platform do you use?
   Android
   iOS
   Windows Phone
   I have mobile phone, not smartphone
   Other: _____

8. What desktop operating system do you use at work?
   Windows
   OSX
   Linux / UNIX-like
   Other: _____

9. What IM apps do you already use?
   Skype
   WhatsApp
   Telegram
   WeChat
   Viber
   LINE
   Google Hangouts
   Silent Phone / Silent Text
   Signal
   ICQ
   Facebook Messenger
   Vkontakte messages
   I use only e-mail apps
   I use only SMS
   Other: _____

10. Approximately how long have you been using an IM client?
    Less than a year
    1 to 2 years
    2 to 5 years
    More than 5 years

11. Do you agree to use new application?
    Scale from 1 to 5, 1 is ‘Don't want to learn a new app’, 5 is ‘Agree to use new app

12. Is it important to you to have a secure connection to the Internet?
    Scale from 1 to 5, 1 is ‘Not at all’, 5 is ‘Very important’

13. Is it important to you to have a secure connection while communicating?
    Scale from 1 to 5, 1 is ‘Not at all’, 5 is ‘Very important’

14. Is it important to you to have a secure communication at work?
    Scale from 1 to 5, 1 is ‘Not at all’, 5 is ‘Very important’

6.2 Full table for the comparison of instant messengers

See attached file.