IRSTI 50.09

O. Baimuratov[1], B. Ziyat[1]
[1]Suleyman Demirel University
Almaty, Kazakhstan

COMPARATIVE ANALYSIS BETWEEN TELEGRAM AND WHATSAPP

Absrtact. This paper presents the results of a comparative analysis between Telegram and WhatsApp. The main attention was paid to their application, which determines their relevance to users, security, MTProto mobile protocol access, end-to-end encryption, data security and functionality.

The leading social networks are usually available in multiple languages and enable users to connect with friends or people across geographical, political or economic borders. Approximately 2 billion internet users are using social networks and these figures are still expected to grow as mobile device usage and mobile social networks increasingly gain traction.

Key words: Messenger, WhatsApp, Telegram, users, social network, statistics, security, end-to-end encryption, MTProto Mobile protocol.

***

Аңдатпа. Бұл мақалада Telegram және WhatsApp арасында салыстырмалы талдау нәтижелері ұсынылған. Негізгі назар оларды қолдануға, қауіпсіздікке, MTProto протоколына, end-to-end шифрлауға, деректерді қорғау және функционалдығына.

Белгілі әлеуметтік желілер бірнеше тілде қол жетімді болуы және пайдаланушылар географиялық, саяси немесе экономикалық шекараларын алмағанда достарымен басқада адамдармен қарым-қатынас жасауға мүмкіндік беретіні анық. Шамамен 2 млрд интернет пайдаланушылар әлеуметтік желілерді пайдалануда, сондай-ақ мобильдік құрылғылар мен ұялы әлеуметтік желілерді пайдалану дамуда кезеңінде.

Кілт сөздер: шифрлау, WhatsApp, жеделхат, пайдаланушылар, әлеуметтік желі, статистика, қауіпсіздік, MTProto Мобильді хаттама.

***

Аннотация. В данной статье представлены результаты сравнительного анализа между Telegram и WhatsApp. Основное внимание было уделено их применению, которое определяет их значимость для пользователей, их безопасности, доступа мобильного протокола MTProto, end-to-end шифрования, защиты данных и функциональности.

Ведущие социальные сети, как правило, доступны на нескольких языках и позволяют пользователям общаться с друзьями или другими людьми без учета географических, политических или экономических

границ. Около 2 миллиардов интернет-пользователей используют социальные сети, и эти показатели по-прежнему будут расти, так как применение мобильных устройств и мобильные социальные сети все больше и больше набирают обороты.

Ключевые слова: пользователи, социальная сеть, статистика, безопасность, сквозное шифрование, протокол MTProto Mobile.

Introduction and History

Instant messaging, instant messaging - instant messaging, online program consultants and client software for messaging in real time via the Internet. Can send text messages, sounds, images, videos, and take actions, such as a joint or a drawing game. Many of these programs, customers can apply for the organization of group text chat or video conferencing.

The Beginnings of Telegram

Behind Telegram stand the brothers Nikolai and Pavel Durov, exiled Russian-born billionaires, previously famous for the Facebook clone Vkontakte (now VK). Pavel Durov had to leave Vkontakte in 2014 over a dispute about handing over Ukrainian protestersz user data. Consequently, the brothers left Russia for Berlin, where they founded Telegram [1].

The Beginnings of WhatsApp

Brian Acton and Jan Koum founded Whatsapp in 2009, to publish quick status updates, similar to those on Facebook. Instant messaging, instant messaging - instant messaging, online program consultants and client software for messaging in real time via the Internet [2]. Can send text messages, sounds, images, videos, and take actions, such as a joint or a drawing game. Many of these programs, customers can apply for the organization of group text chat or video conferencing. Though it was the messaging feature bundled in version 2 that boosted user numbers and made the app a huge success. In February 2014 Facebook bought WhatsApp for US$19 billion, and now they want to integrate it into their internet.org vision.

Let’s find out which messenger service is better. And do a detailed comparison to get a more clear idea of the difference between Telegram and WhatsApp.

Quick Stats

Telegram:

1 Founded in 2013, the app was initially downloaded 100,000 times[3]

2 In March 2014, the app hit 35m monthly active users[3]

3 By 2015, Telegram had 62m active monthly users[4]

4 In December 2015, following the ban of WhatsApp in Brazil, many of the country's users swapped to Telegram[5]

5 The app remains free to download and use, hence it does not generate revenue[6]

6 Its security encryption has been much praised[7]

7 Telegram's founders are facing national security allegations in the fight against ISIS[8]

WhatsApp:

1. WhatsApp Inc raised $250,000 in seed funding on October 2009[9]
2. Series A funding from Sequoia Capital of $8m in April 2011[9]
3. Series C funding by Sequoia Capital in July 2013 at $50m[9]
4. As of September 2015, the app has 900m active monthly users[10]
5. It was acquired by Facebook in February 2014 for $19bn[11]
6. t's average user value is $42[12]
7. Citigroup has forecast that WhatsApp could generate revenue of $1bn by 2017[13]
8. India and South Africa are top markets for WhatsApp[14]

Statistics and Revenue

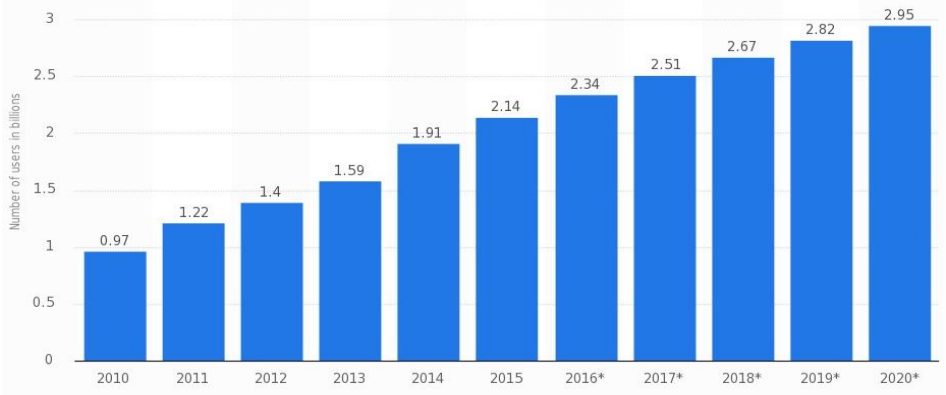

Fig.1 Number of social network users worldwide from 2010 to 2020 (in billioons) [15]

This statistic shows the number of social media users worldwide from 2010 to 2016 with projections until 2020. In 2018, it is estimated that there will be around 2.67 billion social media users around the globe, up from 1.91 billion in 2014 [15].

Social media users

Social media penetration worldwide is ever-increasing. In 2016, 68.3 percent of internet users were social media users and these figures are expected to grow. Social networking is one of the most popular online activities with high user engagement rates and expanding mobile possibilities. North America

ranks first among regions where social media is highly popular, with an social media penetration rate of 59 percent. In 2016, more than three quarters of the United States population had a social media profile. Overall, U.S. users spend more than 216 weeks minutes on social media via smartphone, 53 weekly minutes via PC, and 50 minutes per week on social networks via tablet devices.

Social networks not only enable users to communicate beyond local or social boundaries, but also offer possibilities to share user-generated content like photos and videos and features such as social games. Social advertising and social gaming are two major points of revenue for social networks.

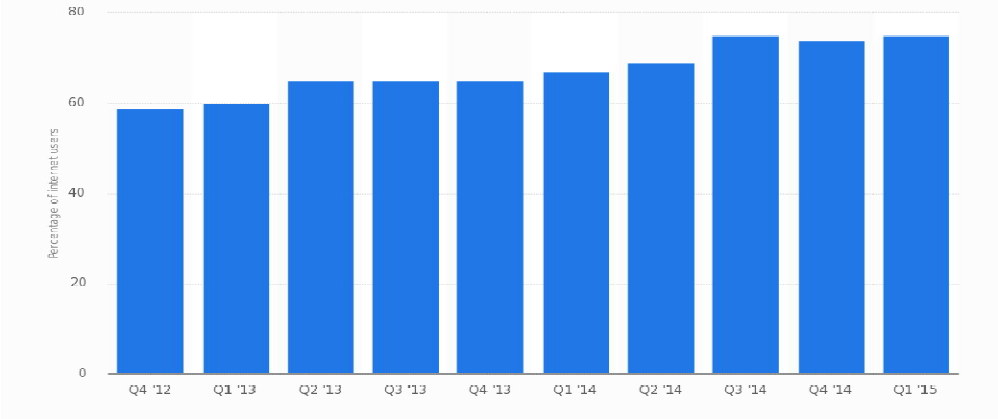

Fig.2 Global mobile messaging usage penetration from 4th quarter 2012 to 1st quarter 2015 [16]

This statistic presents the global mobile instant messaging usage penetration among internet users worldwide. As of the first quarter of 2015, 75 percent of internet users worldwide had accessed the messaging services on mobile [16].

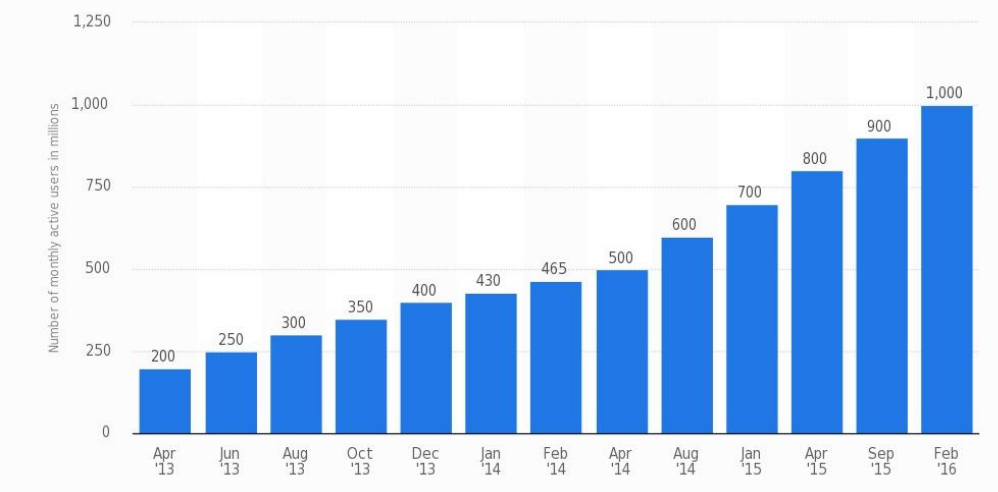

Fig.3 Number of monthly active WhatsApp users worldwide from April 2013 to February 2016 (in millions) [17]

This statistic shows a timeline with the amount of monthly active WhatsApp users worldwide as of February 2016. As of that month, the mobile messaging app announced more than 1 billion monthly active users, up from over 700 million in January 2015. The service is one of the most popular mobile apps worldwide [17].

WhatsApp is a cross-platform instant messaging service for smartphones that relies on the internet for the transmission of messages. Based on a low-cost subscription model, WhatsAppis a cheap alternative to carrier-billed text messaging via SMS, especially for international or group messaging. The mobile messaging app enables users to share text, image and video messages – the service handles more than 600 million photo and 64 billion overall messages every day. In the United States, the daily engagement rate among Android WhatsApp users was 36 percent.

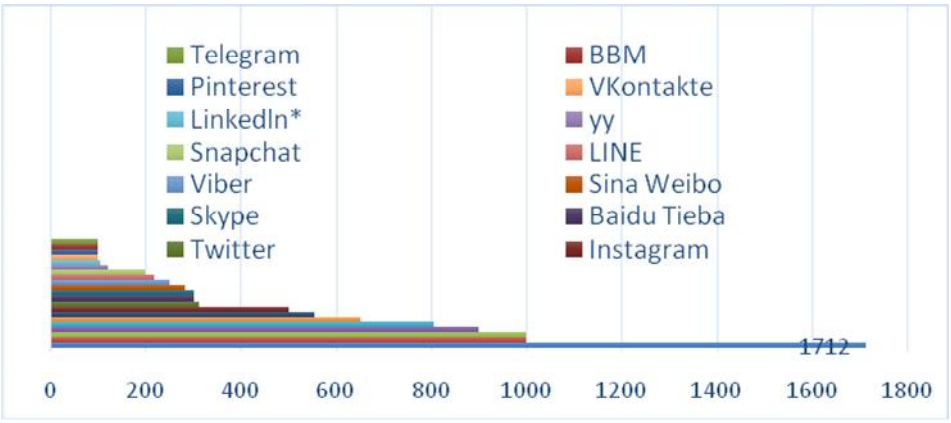

Fig.4 Most famous social network sites worldwide as of September 2016, ranked by number of active users (in millions) [18]

This statistic provides information on the most popular networks worldwide as of September 2016, ranked by number of active accounts. Market leader Facebook was the first social network to surpass 1 billion registered accounts and currently sits at 1.71 billion monthly active users. Eighth-ranked photo-sharing app Instagram had over 500 million monthly active accounts. Meanwhile, blogging service Tumblr had more than 555 million active blog users on their site [18].

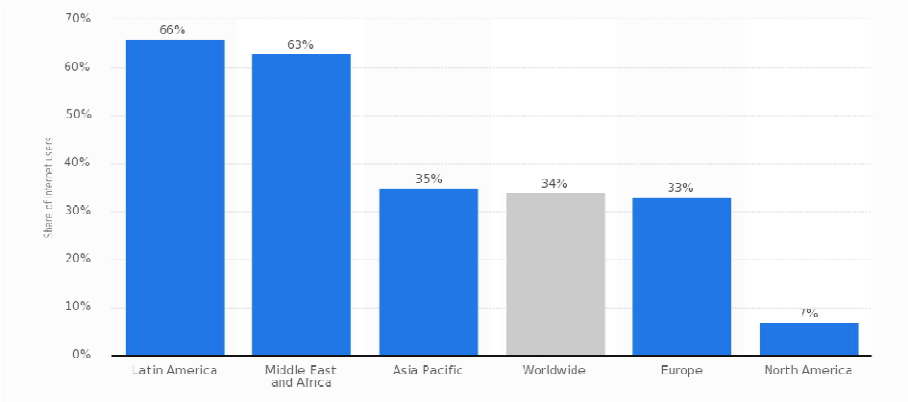

Fig.5 Usage penetration of WhatsApp in selected global regions as of 4th quarter 2015 [19]

This statistic gives information on the global WhatsApp messenger audiences reach in selected global regions. As of the fourth quarter of 2015, 66 percent of internet users in Latin America had used the mobile app within the past month [19].

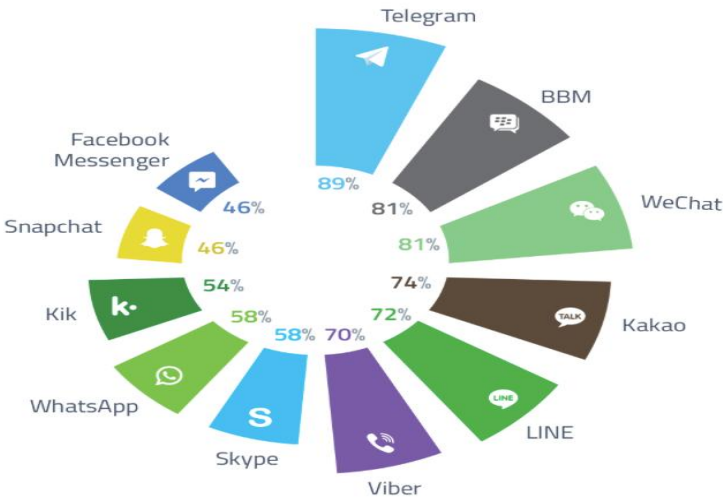

Fig.6 Interest in money transfer features % active user interested in money transfer features on mobile messaging apps [20].

With many of the world's messaging apps turning themselves into platforms where users can do far more than simply chat with each other, Tuesday's blog assesses levels of interest in using in-app money transfer features.

If we look at mobile IM users in key digital markets like the US and UK, it is those on Telegram, BBM and WeChat who express the most enthusiasm – with more than 8 in 10 in each group saying they are very or quite interested in this function.

It's hardly surprising that apps with their origins in APAC score particularly well: on some of these services, the ability to transfer money has been around for a long time. And while it's certainly striking that Kik, Snapchat and Facebook Messenger come at the bottom of the table, it's still around half of their respective user bases who express an interest in a money-transfer service – indicating the size of the potential audience for Snapcash as well as Facebook Messenger's rival feature [20]

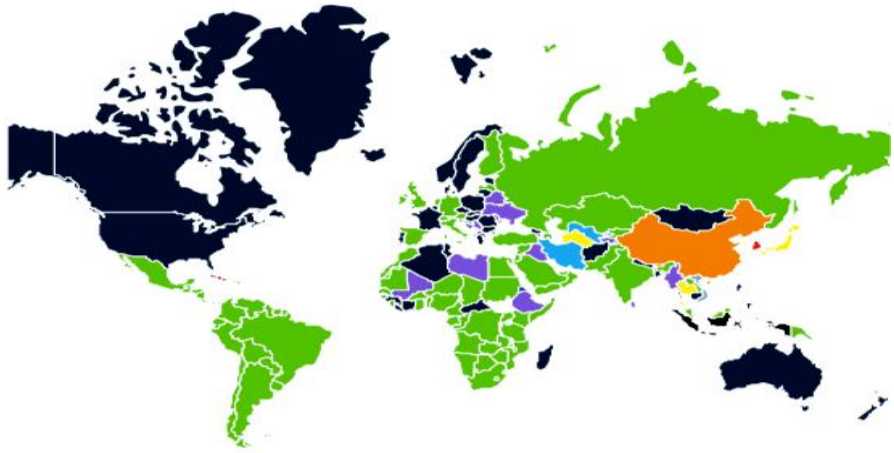

Fig.7 Most popular messaging app in every country [21].

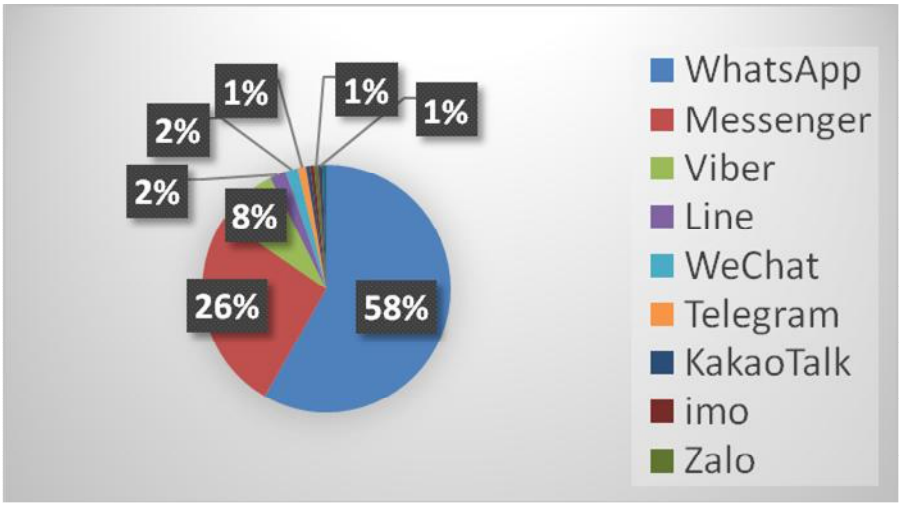

Fig. 8 The World of Messaging Apps

Using Android data from 187 countries, we were able to determine the most popular messaging app all over the world. In fact, in almost every country in the world, a messaging app is the most used app overall.

Of the 187 countries that SimilarWeb examined, WhatsApp was the world leader claiming 109 countries, or 55.6% of the world. WhatsApp's countries include Brazil, Mexico, India, Russia, and many other countries in South America, Europe, Africa, Asia, and Oceania.

Facebook's Messenger app came in second overall, claiming 49 countries including Australia, Canada, and the U.S. After Messenger, Viber was the only other messaging app to claim 10 or more countries. The app shows strong popularity in Eastern Europe, and is the top app in Belarus, Moldova, Ukraine, and others. In fact, as of April 2016, Viber was installed on 65% of all Android devices in Ukraine and was used for an average of 16 minutes a day. Viber's popularity also reaches other parts of the world including countries such as Iraq, Libya, and Sri Lanka.

Line, WeChat, and Telegram are 3 other messaging apps claiming multiple countries with China, Iran, and Japan representing countries using one of these apps. Japan's obsession with Line is well documented and in a recent post, we discovered that not only is Line the most popular app in Japan, people who have it use it for an average of 40 minutes a day!

Finally, apps that only claimed one country include KakaoTalk in South Korea, imo in Cuba, Zalo in Vietnam, ChatOn in Eritrea, and BBM in Indonesia [22, 33].

IV. Security

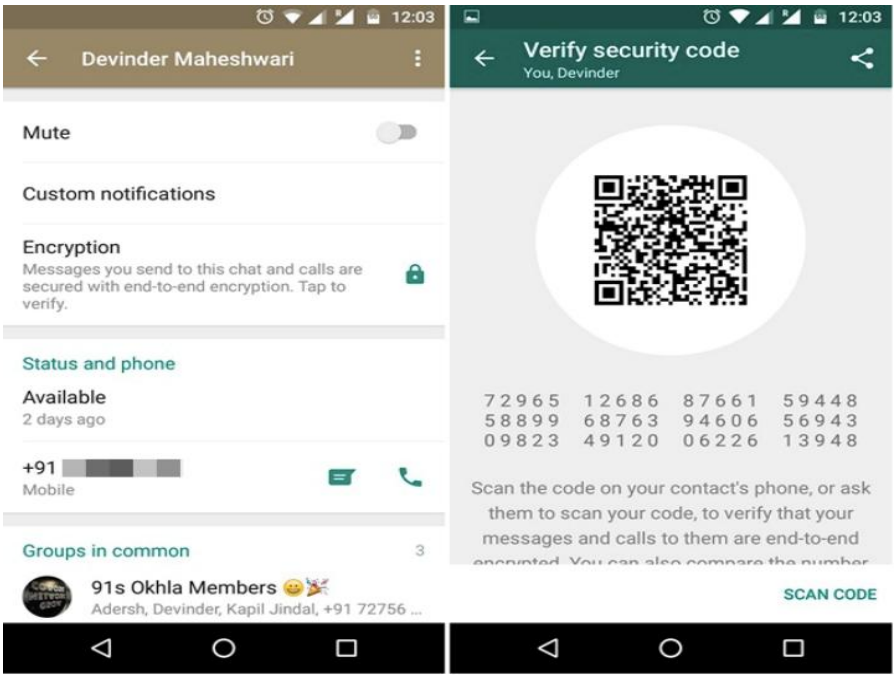

Fig. 9 Encryption of Telegram and WhatsApp

Telegram uses a self-developed protocol, called MProto. Telegram has been heavily criticized for creating its own standard, rather than making use of something else. MProto is not entirely new, however (it makes use of the AES and RSA standards), and OpenWhisper Systems (the standard WhatsApp has incorporated) is also a new development.

ExpressVPN is not cryptographers, but it appears the MProto protocol has yet to be broken. It's also open-source, like all Telegram apps, so anyone is free to try to break it. In fact, Telegram has repeatedly offered large bounties (the current one is US$ 200,000 in Bitcoin) to anyone who can successfully break the standard, though Moxie Marlinspike, the creator of OpenWhisper Systems, has called the prize "rigged" in his blog [23].

Telegram's encryption cipher is certainly very fast and efficient, and encrypted messages can be sent when all other apps fail due to slow Internet connections. Telegram also changes keys every week, or after 100 messages, to provide perfect forward secrecy. Perfect forward secrecy ensures that if your phone were ever to get hacked and the encryption keys are stolen, your deleted messages could not be decrypted.

The big difference lies not in what encryption protocols are being used, but how they are applied. WhatsApp automatically encrypts all your messages, and there is no option to send an unencrypted message. This is a huge difference compared to Telegram's encryption, where you have to select

“Secret Chat” to initiate a secure conversation. Many people don’t do this, either because it’s an extra step, or because they don’t understand the necessity.

Without encryption, chats are vulnerable to interception and surveillance, even more so on Telegram, where messages are stored until you delete them. WhatsApp, on the other hand, does not store messages, it only forwards them to your device. Even group chats are encrypted in WhatsApp.

In both platforms you should compare encryption keys to make sure your chats are not being attacked, for example by a man-in-the-middle. In WhatsApp, this is done on a person-per-person basis, and you only need to recheck the key if one of you reinstalls the app, or gets a new device. In Telegram each chat has its own key. This is great in theory, as it allows the creation of individual secure lines among trusted devices, but doesn’t work well in practice. Each time you start a new secret chat, you need to verify the other person’s identity again.

V. Encryption of WhatsApp

The main safety rating messengers forms Electronic Frontier Foundation (EFF). His website is constantly updated table where messengers get from one to seven points, depending on the number of tests passed.

According to this table have WhatsApp was rated two out of seven to November 2014: messenger encrypt messages during transmission and in an independent security audit took place during the past years. However, on the day of inclusion endpoint encryption EFF issued chats WhatsApp six of seven points.

New WhatsApp encryption protocol worked Open Whisper Systems (OWS) - developer messenger Signal, recommended the use of Edward Snowden. In December 2015 the founder Telegram Pavel Durov even entered into a public argument with the head of OWS Moxie Marlinspike: he supported the statement that the Telegram stored on the server unencrypted message (it is not), and Durov in response accused the supporters of this view in the "proplachennoy nonsense ". However, working together with WhatsApp Marlinspike year and a half has brought a popular messenger standards typical of the favorite methods of communication paranoid. Extra points are given EFF for the opportunity to verify the identity of the interlocutor reconciliation of security keys, frequent change of keys (if one of them stolen, decipher only a small part of the correspondence), as well as detailed documentation on the use of terminal encryption.

Table 1. The Secure Messaging Scorecard, EFF

Telegram	Encrypted in	Encrypted so the provider	Can you verify contact	Are past comms open to	Is the code open to	Is security deston properly	Has there been any recent code

	transit?	can't read it?	identitles?	independent review?	indepen dent review?	documente d?	audit?
Telegram	+	−	−	−	+	+	+
Telegram (secret char)	+	+	+	+	+	+	+
Threema	+	+	+	+	−	+	+
Viber	+	−	−	−	−	+	+
Virtu	+	−	−	−	−	+	+
WhatsApp	+	+	+	+	−	+	+

For example (in Table 1), in secret chats Telegram in this table are rated seven out of seven, but conventional - four out of seven. It is believed that the messages in the chat rooms are available for standard decoding Telegram itself, and therefore, potentially, and read by third parties - although Telegram claim that data are not transferred to anyone. Confirm the identity of the interlocutor with the key in such chat rooms cannot be, and it may lead to theft of decoding the entire message history [24].

VI. Technically work of end-to-end encryption in WhatsApp

To communicate with another WhatsApp user, a WhatsApp client first needs to establish an encrypted session. Once the session is established, clients do not need to rebuild a new session with each other until the existing session state is lost through an external event such as an app reinstall or device change.

To establish a session:

1. The initiating client ("initiator") requests the public Identity Key, public Signed Pre Key, and a single public One-Time Pre Key for the recipient

2. The server returns the requested public key values. A One-Time Pre Key is only used once, so it is removed from server storage after being requested. If the recipient's latest batch of One-Time Pre Key has been consumed and the recipient has not replenished them, no One-Time Pre Key will be returned

3. The initiator saves the recipient's Identity Key as Irecipient, the Signed Pre Key as Srecipient, and the One-Time Pre Key as Orecipient

4. The initiator generates an ephemeral Curve25519 key pair, Einitiator

5. The initiator loads its own Identity Key as Iinitiator

6. The initiator calculates a master secret as master_secret = ECDH(Iinitiator, Srecipient) || ECDH(Einitiator, Irecipient) || ECDH(Einitiator, Srecipient) || ECDH(Einitiator, Orecipient) If there is no One Time Pre Key, the final ECDH is omitted

The initiator uses HKDF (Extract-and-Expand Key) to create a Root Key and Chain Keysfrom the master_secret Exchanging Messages

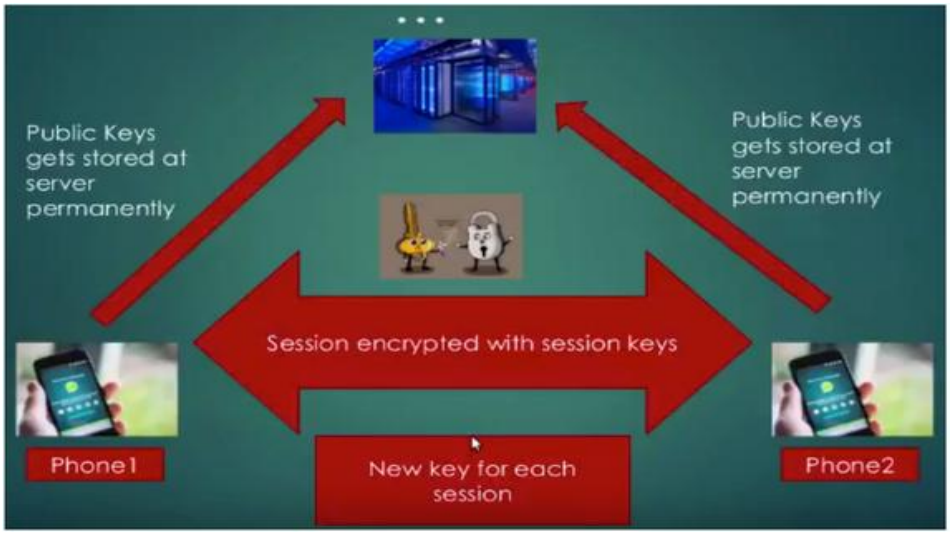

Fig. 9. The Scheme of WhatsApp encryption [25]

Once a session has been established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication.

The Message Key changes for each message transmitted, and is ephemeral, such that the Message Key used to encrypt a message cannot be reconstructed from the session state after a message has been transmitted or received.

The Message Key is derived from a sender's Chain Key that "ratchets" forward with every message sent. Additionally, a new ECDH agreement is

performed with each message roundtrip to create a new Chain Key. This provides forward secrecy through the combination of both an immediate “hash ratchet” and a round trip “DH ratchet.”

What happens after this process is each device on one side A and B have exchanged private keys which are unique for each session and each user. If we compare this situation to keys from your home, it means each time you go home you will have a new key in your pocket, but all exchange will be done automatically without you being involved [25].

The image above, sums up the WhatsApp encryption scheme. Public keys linked with a users’ identity are stored on the server. Every message exchanged between two users is encrypted using a new key - uses a key chain/ratchet mechanism.

The best feature is that, even if encryption keys from a user’s device are ever physically compromised, they cannot be used to go back in time to decrypt previously transmitted messages. => Provides Perfect Forward Secrecy. Without going into thorough details, the key derivation algorithm produces keys, which aid in providing confidentiality (no one else other than the two parties, can see your messages) and authentication (proving you are who you say you are).

VII. MTProto Mobile Protocol

The protocol is designed for access to a server API from applications running on mobile devices. It must be emphasized that a web browser is not such an application.

The protocol is subdivided into three virtually independent components:

1. High-level component (API query language): defines the method whereby API queries and responses are converted to binary messages

2. Cryptographic (authorization) layer: defines the method by which messages are encrypted prior to being transmitted through the transport protocol.

Transport component: defines the method for the client and the server to transmit messages over some other existing network protocol (such as, http, https, tcp, udp).

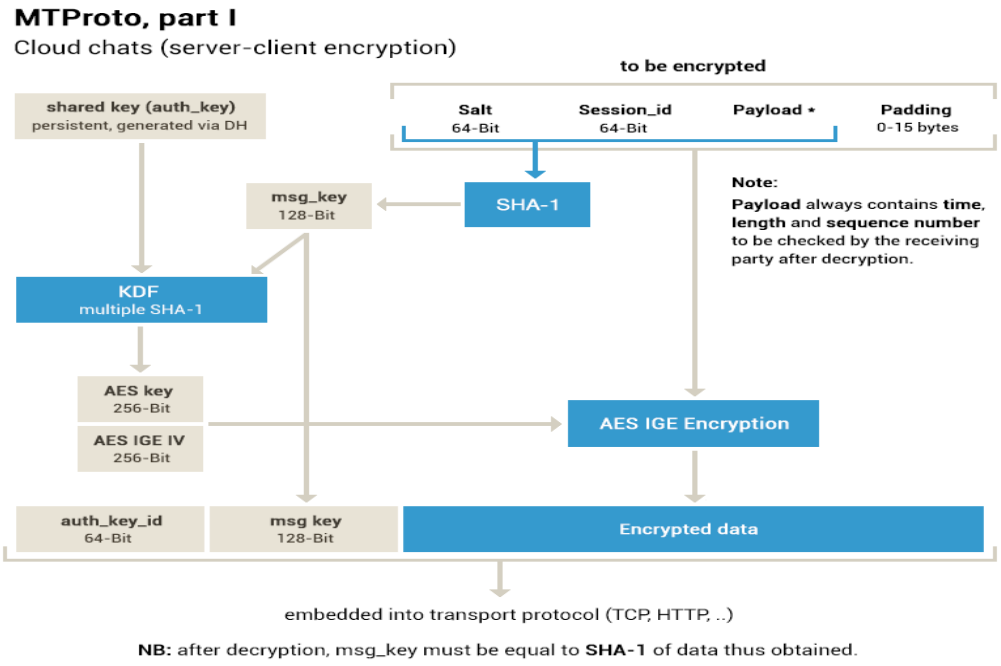

Fig. 10.Cloud chats (server-client encryption) [26]

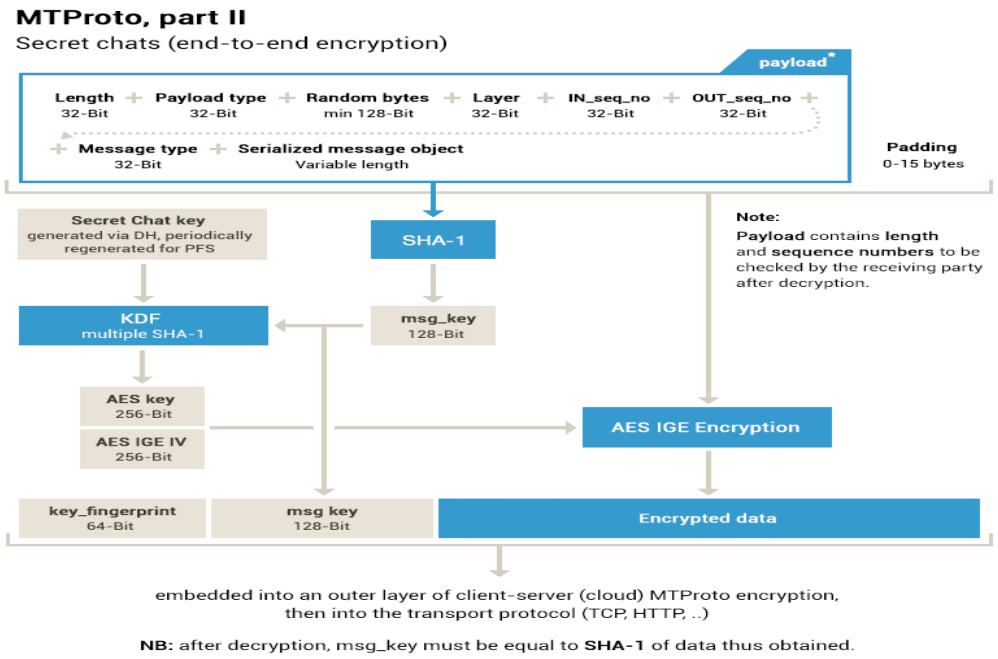

Fig. 11. Server chats (end-to-end encryption) [26]

In MTproto, partII the Secret Chats are one-on-one chats wherein messages are encrypted with a key held only by the chat's participants. Please note that the schema for end-to-end encrypted Secret Chats is different from what is used for cloud chats.

Sending and Receiving Messages in a Secret Chat

Serialization and Encryption of Outgoing Messages

A TL object of type DecryptedMessage is created and contains the message in plain text. For backward compatibility, the object must be wrapped in the constructor decryptedMessageLayer with an indication of the supported layer (starting with 8).

The TL-Schema for end-to-end encrypted messages contents is represented .

The resulting construct is serialized as an array of bytes using generic TL rules. The resulting array is padded at the top with 4 bytes of the array length not counting these 4 bytes.

A message key, msg_key, is computed as the 128 low-order bits of the SHA1 of the data obtained in the previous step.

The byte array is padded with random data until its length is divisible by 16 bytes.

An AES key and an initialization vector are computed (key is the shared key obtained during Key Generation, x = 0):

1. sha1_a = SHA1 (msg_key + substr (key, x, 32));
2. sha1_b = SHA1 (substr (key, 32+x, 16) + msg_key + substr (key, 48+x, 16));
3. sha1_c = SHA1 (substr (key, 64+x, 32) + msg_key);
4. sha1_d = SHA1 (msg_key + substr (key, 96+x, 32));
5. aes_key = substr (sha1_a, 0, 8) + substr (sha1_b, 8, 12) + substr (sha1_c, 4, 12);
6. aes_iv = substr (sha1_a, 8, 12) + substr (sha1_b, 0, 8) + substr (sha1_c, 16, 4) + substr (sha1_d, 0, 8);

Data is encrypted with a 256-bit key, aes_key, and a 256-bit initialization vector, aes-iv, using AES-256 encryption with infinite garble extension (IGE). Encryption key fingerprint key_fingerprint and the message key msg_key are added at the top of the resulting byte array[23, 26-27, 31-33].

Encrypted data is embedded into a messages.sendEncrypted API call and passed to Telegram server for delivery to the other party of the Secret Chat.

Decrypting an Incoming Message

The steps above are performed in reverse order.

When an encrypted message is received, you must check that msg_key is in fact equal to the 128 low-order bits of the SHA1 hash of the decrypted message.

If the message layer is greater than the one supported by the client, the user must be notified that the client version is out of date and prompted to update[27]

VIII. Getting Started: Which Has the Sign up Process

For WhatsApp, you can only sign up through a mobile phone app, while Telegram lets you sign up anywhere, even with their web app.

But both Telegram and WhatsApp use your phone number for authentication. This is convenient at first but leaves serious security concerns. A hacker could take over your account by diverting text messages to their own number by either tricking your mobile phone provider or even colluding with them. The latter is especially of concern if your adversary is your local government.

For the encrypted WhatsApp, this will allow hackers to impersonate you, but with Telegram, someone could gain access to all your unencrypted chats and group chats .

Though WhatsApp has superior encryption, Telegram has the option to set a secondary password, which is effectively two-factor authentication. A hacker will need not only access to your phone number but also a password to get to your contacts [28].

Giving users no option other than signing up with a number is not a good practice. Phone numbers can easily be linked to an identity through location, and many countries require you to show ID when buying SIM cards.

IX. Which Has the Best Download Options

Telegram’s apps are all open-source, which means you can build them yourself, rather than downloading them from the app stores. You can modify the apps, and researchers can look through them to find errors in the implementation of security features. You can also build a Telegram integration for your own application, which makes it more accessible to people who do not have access to official app stores (for example if their country blocks them), but it also means a susceptibility to backdoored or malicious versions [13,29].

Open-source is pretty awesome, and Telegram impresses further with its wide range of supported platforms. There are the usual such as iOS, Android, and Windows Phone, but there is also browser apps for Firefox and Chrome OS, a Pidgin plugin, desktop apps, and even a Command Line Interface! Sadly, though, the Windows and Linux apps are just wrapped

versions of the browser app (Webogram), which does not support end-to-end encryption.

WhatsApp also has a Windows and Mac app, but it primarily focuses on mobile phones, where it supports older systems like Symbian or Blackberry. WhatsApp is far more restrictive and has in the past shut down independent implementations, such as a Pidgin plugin [30-32].

Table II. Pros and Cons between WhatsApp and Telegram

	WhatsApp	Telegram
ros	Calls Backup chats Massive user base End to end encryption everywhere	Secure Overall more feature-rich Bots and great file sharing Better platform compatibility
Cons	Limited file sharing Not as feature-rich as Telegram	No calls support or ability to backup chats Lacks user base

Conclusion

As a result of the analysis on the basis of statistical data presented in Figure 1-11, Table I,II and 1-32 the basic sources advantage and disadvantages Telegram and WhatsApp.

The one-billion-people app has brought end-to-end encryption to the masses, and ExpressVPN thinks it may be the only big platform that does encryption right. Unfortunately, WhatsApp struggles to become more than a dull pipe for messages, and some users might expect more. The fact that users are confined to a single device/app feels like the biggest barrier.

Telegram Has More Features and Is Open Source. The platform impresses through being open-source, easily accessible for designers (stickers) and developers (bots), and boasts a massive line-up of apps for all kinds of platforms. All apps ExpressVPN tried felt fast and beautifully integrated with the operating systems they were built for. While far from anonymous, ExpressVPN feels you are a bit more in control of your identity and contacts. The biggest problem is the lack of End-to-end encryption by default.

The Telegram messages in normal chat is encrypted with the key on the server of the messenger, so the user's encryption key can be transferred to other devices (conventionally, his message is not read unless hacked server Telegram). This allows the use Telegram on any number of devices simultaneously.

The WhatsApp with end encryption is no such possibility. When you enter a phone number (WhatsApp no logins) on the first smartphone at the same time cut off the first session of the smartphone, and you cannot continue

the conversation. The same problem with the "secret chats" in the Telegram: if people started encrypted conversation on one device, the second he did not continue - it is necessary to create a new one[10].

In most cases, the ability to use Messenger on multiple devices - this is a luxury for ordinary people a maximum of one smartphone. Another thing, when the chat need to go from your computer: we Telegram there are special customers, while WhatsApp - tricky web version, which connects via the Internet to a running application on your smartphone (it should also at this point to have access to the network).

Another thing - the history of correspondence: it is important, if you change the device periodically (you break, the transition to new). By default, WhatsApp does not save her, you can enable the preservation of the phone memory, but how to extract it from the message, it is not clear from the application interface. Correspondence can be synchronized with the cloud service: on Android - with Google Drive, on iOS - with iCloud. But how to move correspondence with iOS to Android or vice versa, it is not clear (probably impossible), and even using the same account (for example, Google Drive) between the two devices, the story is not tolerated.

References:

1 Bhasin, B. Integration of Information and Communication Technologies in Enhancing Teaching and Learning // Contemporary educational technology. – 2016. – vol. 3(2) – P. 130-140

2 Shukla, A., Shrivastava, P., Yadav, P. and Kumar, A. Backup manager - An Android application for storing messages and apps information online // IEEE conference materials. – December, 2015. – P. 120-220

3 Job, J., Naresh V., Chandrasekaran, K. A modified secure version of the Telegram protocol (MTProto) // IEEE conference materials. – January, 2016. – P. 32-86.