Oleh HARASYMCHUK[1], Viktoriia TYSHCHENKO[2], Ivan OPIRSKYY[3], Vasyl RAMSH[4]

Opiekun naukowy: Oleh HARASYMCHUK[1]

DOI: https://doi.org/10.53052/9788366249868.04

ANALIZA PODEJŚĆ DO ZWIĘKSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W KOMUNIKATORACH INTERNETOWYCH

Streszczenie: Przedstawiono trendy w rozwiązaniach zwiększających bezpieczeństwo w komunikatorach internetowych. Oferowane są najbardziej efektywne podejścia do rozwiązywania problemów bezpieczeństwa na podstawie badań tematycznych aplikacji do obsługi wiadomości błyskawicznych oraz określane są zalety ich realizacji.

Słowa kluczowe: dane, wiadomości błyskawiczne, ochrona danych osobowych, ataki, zagrożenia, analiza bezpieczeństwa, szyfrowanie

ANALYSIS OF SOLUTIONS TO INCREASE THE SECURITY OF PERSONAL INFORMATION IN INSTANT MESSAGING SYSTEMS

Summary: Trends in solutions to increase security in instant messaging services have been presented. The most effective approaches to solving security problems have been defined base on instant messaging applications case studies as well as the advantages of their realization.

Key words: data, instant messaging, personal information protection, attacks, threats, security analysis, encryption.

1. Introduction

The availability, low cost, and ease of use of Instant Messaging (IM) have led to their growing popularity in both face-to-face and corporate communication. It has evolved

[1] PhD, Lviv Polytechnic National University, Associated Professor of Information Protection Department, oleh.harasymchuk@gmail.com
[2] Lviv Polytechnic National University, student of Information Protection Department, vikatishtshenko@gmail.com
[3] DSc, Lviv Polytechnic National University, Professor of Information Protection Department, iopirsky@gmail.com
[4] PhD, Separated Subdivision of National University of Life and Environmental Sciences of Ukraine Berezhany agrotechnical institute, Associated Professor of Energy and Automatics Department, ramsh_v@ukr.net

from a means of communication between people into a means of obtaining information and an incredibly powerful marketing tool. Bots played a significant role in this. IM is a telecommunication service for exchanging real-time text messages over the Internet. Today, nearly 2.5 billion people worldwide use messaging programs in their daily lives. Nowadays, IM services allow not only exchanging text messages, but also to make calls, video calls and transfer files.

However, the disadvantage of this convenience is the risk of leakage of private information of service users. In general, client-server architecture is common for modern instant messaging systems. By managing connections between network users, the server has the theoretical ability to store communication history and provide access to it to third parties.

Instant messaging exceeds e-mail, offering an immediate and clear solution to problems that may have gone unnoticed in the "incoming" folder. Messengers have become more popular than social networks. Some of the main advantages of instant messaging programs over social networks include high engagement rates, automation of communication, and personalized contacts. That is why almost every social network today has its own messenger.

One of the main features of many instant messaging clients is the property that shows if the person is online and connected through the selected service. As technology has evolved, many instant messaging clients have added support for more than just text messaging, allowing for file transfer, image and voice messaging, and location sharing. In addition, the revelation of mass surveillance by NSA employee Edward Snowden has led to a demand for safe communication based on confidentiality.

Instant messaging services are integrated into our daily lives in both personal and business contexts as a convenient form of communication. Although these programs make communication quick and easy, one should be aware of vulnerabilities to various security threats when using them. In addition, different application developers have various security standards.

Therefore, it is significant to determine the most effective countermeasures for information security that can be used in IM to minimize or mitigate threats to personal information.

1.1. Analysis of threats to instant messaging services and solution trends

Typically, instant messaging users need to know each other's username or nickname to start an instant messaging session or add them to their contact list or friends list. Once the designated recipient is identified and selected, the sender opens a chat window to start the session.

For instant messaging to work as intended, both users must be online simultaneously, although almost all instant messaging platforms now allow asynchronous interaction between users on and off the Internet. If offline messaging is not supported, trying to exchange instant messages with an unavailable user will result in a warning stating that the transfer cannot be completed.

Upon receiving an instant message, the application alerts the recipient with a window containing an incoming message. Or, depending on the user's settings, a message may appear in the window stating that the IM has been received with a request to accept or reject it. Many instant messaging clients also notify the user with an audible signal.

The user can also receive a visual notification, a demonstration of the chat window or its icon on the taskbar when a message arrives.
Although in the past messaging clients were often based on closed (proprietary) protocols requiring both users to use the same communication software, the adoption of open standards has become more common. It has led to the development of cross-platform messengers such as Pidgin and Trillian.
Another crucial shift in the messaging system took place in the way of accessing and delivering messages. Formerly instant messaging was a client that needed to be downloaded and installed. Now instant messaging is more common as a feature in another web or cloud service - such as Facebook, Gmail and Skype - or as a mobile application, such as WhatsApp Messenger.

1.2. IM salient features

We can identify the following characteristics that are significant for technological purposes and will be important in the protection of IM [1]:
1. Simultaneity. IM is a real-time or "synchronous" form of communication, so there is a real-time risk related to it.
2. Recording. Instant messaging is a form of written communication that means there are logs and sessions that can be recorded. This is exactly the same as email, although in a P2P connection it can be difficult to use.
3. Nonrepudiation. IM typically involves dialogue and the appearance of nonrepudiation by virtue of exchange, although inherent nonrepudiation is not typical of most IM infrastructures.
4. Lack of confidentiality and integrity. There is no guarantee that sessions are private or unchanged in most messaging infrastructures without effective encryption solutions.
5. Availability. Most companies do not have guaranteed service level agreements on availability, and yet they depend on IM, consciously or unconsciously, and bear the cost of maintaining the service when it is down.

1.3. Threats to the IM

In the context of IM, there are obvious threats, internal and external, as well as unintentional and malicious. These different threats require different countermeasures.
Figure 1 shows a grid of groups of individuals and activities that a security professional will need to consider in the context of IM security [1].

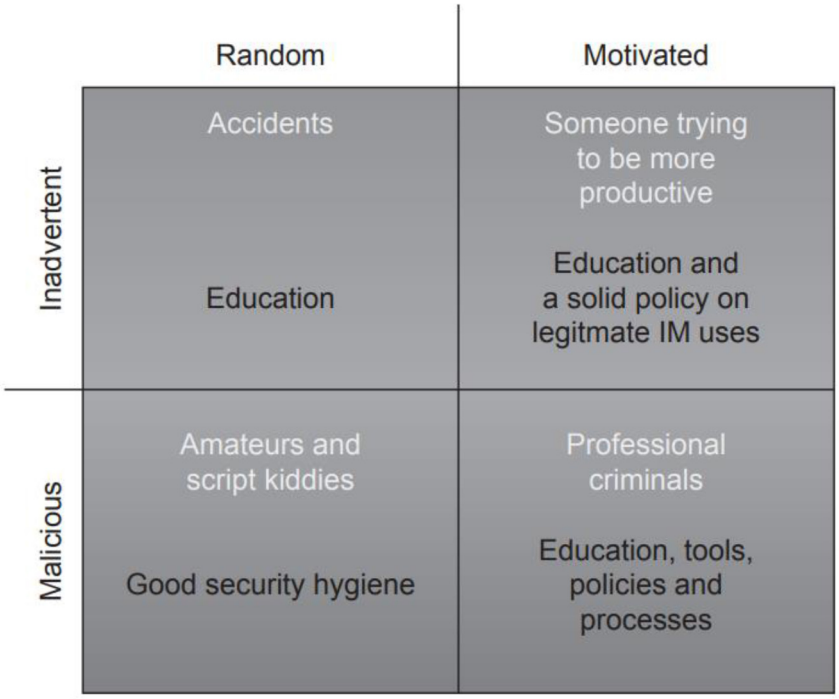

Figure 1. Groups of individuals that may pose a threat and appropriate measures of prevention

The main types of attacks on instant messaging services:

- *Man-in-the-middle attacks* are a class of attacks in which a third party acts as a legitimate or even invisible intermediary. An attacker introduces each instant messaging user to the legal part of the process by actually recording or transmitting information. In the absence of proper authentication and encryption, this attack can be carried out by attackers on a large scale.
- *Attacks due to vulnerabilities*. Add-ons and messaging infrastructure are exposed to vulnerabilities and shortcomings due to improper configuration and implementation. Most of these programs are not as rigorous in the matter of maintenance, support, and bug fixes as other enterprise software programs. As a result, it is crucial to have penetration testing and security audit processes and to establish relationships, if possible, with manufacturers and distributors to maintain the enterprise level.
- *Spread of viruses and worms*. Instant messaging programs are fast becoming a popular method for launching network viruses and worms. The lack of built-in security, the ability to download files, and the recipients' built-in "friends list" create an environment in which viruses and worms can spread quickly.
- *Denial-of-service attacks*. The risk of denial-of-service attacks is very serious for instant messaging programs. DoS/DDoS attacks prevent legitimate users from accessing the network by overusing the network to consume resources, destroy configurations, and modify network components.

- *Phishing and social engineering*. An attack of this kind can be based on usage of trusted logos and context, which seems normal, but is in fact designed to create a vulnerability that can be exploited by a social engineer.
- *Information as a commodity*. Apparently, knowledge of business processes is something that can be turned into profit. The content, value and type of financial transaction are valuable to competitors and speculators. The value of shares rises and falls due to rumours about companies' activities, and accurate information about what is happening can be directly monetized. There are companies, organizations and individuals who launder money and make huge profits from insider information and intellectual property, and criminals are looking for just that information.
- *Data and traffic analysis*. The mere presence of communications is sufficient, in certain circumstances, to indicate significant facts about the business. Whenever possible, artificial levels of traffic and flags of data content to the outside world should be used to mask the nature and timing of communications that contain insider information.
- *Unintentional threats*. Perhaps the most insidious threat is not malicious but unintentional. These include:
a) Leakage of intellectual property (source code, insider information, trade secrets, etc). Although, it should be clarified that with proper deployment such transactions can be securely performed through IM (when they are encrypted and there is proper mutual authentication).
b) Improper use of chat can lead to risks and threats to the business and personal lives of users. In particular, IM is an informal medium. Sending confidential or even compromising information through instant messaging carries the risk of exposing and disclosing it.

1.4. Security analysis and solution trends

Cybersecurity expert Mark Williams has created a table comparing the most popular instant messaging applications [2]. This comparative characteristic makes the following requirements:
- Is encryption enabled by default?
- Is the intelligence functionality built-in?
- Does the application/company collect user data?
- Can the company read the message?
- Does the application allow an additional identification factor?
- Does the application store and/or generate a private key directly on the device?
- Does the application provide the feature of self-destructing messages?
-Was the application/company involved in providing personal data of users to special services?

Table 1 provides recommendations for the use of some instant messaging services [2]. As a result of the comparison, Signal and Wire applications can be recommended for secure messaging and attachment transfer.

Table 1. Recommendations for using some of the most popular instant messaging applications

IM	Can the program be recommended for secure communication?	Main reasons why the program isn't recommended/ Recommended improvements
Facebook Messenger	No	Named an NSA partner in the Snowden investigation. Encryption is not enabled by default. Makes money from personal information. Data is not protected / not all data is protected. There is no independent and recent code audit and security analysis. Closed source code.
Facebook Whatsapp	No	Named an NSA partner in the Snowden investigation. Makes money from personal information. Data is not protected / not all data is protected. There is no independent and recent code audit and security analysis. Closed source code
Telegram	No	Bespoke cryptography. Encryption is not enabled by default. Data is not protected / not all data is protected.
Viber	No	Data is not protected / not all data is protected. There is no independent and recent code audit and security analysis. Closed source code.
Signal	Yes	Remove the mandatory requirement for users to sign up with a mobile number. Provide more comprehensive independent assessments of security/privacy.
Wire	Yes	Further limit metadata storage and logging. Provide more comprehensive independent assessments of security/privacy.

It is important to review the solutions provided in most resent studies in this area in order to solve existing problems, reduce their consequences and meet the needs of user privacy. The following trends can be identified:

- Anonymization. Involves the removal of all identifying or identifiable information from the data to be hidden. When service providers share their data for research purposes, highly confidential information about users can be displayed implicitly or explicitly on social graphics, so there should be an anonymous way to reduce the potential risks for their users. However, the disadvantage of this trend is that it is difficult to prove that these methods are secure compared to traditional cryptographic operations.
- Decentralization. The confidentiality of user data is compromised through central management and storage, as this way the service provider can have full access to users' personal traffic. As a substitute for a centralized approach, peer-to-peer architectures

have provided the basis for decentralized IM to avoid an omniscient service provider. Using a decentralized protocol, messages sent in the program do not pass through the company's servers.
- Privacy management and configuration. Most users are careless about their profile's privacy settings, although almost all IMs provide privacy management settings so users can control what information they want to share and whom they want to join. However, most users are not sufficiently informed about the data they may explicitly or implicitly disclose and the dangers of such disclosure, and generally accept the default privacy settings provided. Research in this area revolves around empowering users to control or facilitate their privacy settings. It is also necessary, in addition to granting the right to privacy settings, to inform users about the consequences of leakage of confidential information.
- Encryption. It is used as a tool to ensure aspects of confidentiality and as a basis for integrity. With encryption, only the person to whom you send your messages can actually read them. Powerful encryption software built into messaging programs means that any third party who intercepts these messages will not be able to read them. In addition, encryption for IM must be end-to-end. Security experts are working on achieving extensive use of end-to-end encryption, which reduces the impact of such attacks. [3]
- Information, legislation and rules. Non-technical research focuses on raising users' awareness of IM privacy issues and compliance by both service providers and users with social norms and established laws. Privacy policies and regulations are not mandatory, and it usually takes time to raise awareness. Laws solve problems after something goes wrong, and technical solutions are used to prevent violations. That is, non-technical solutions can be effective only in combination with technical ones.

2. Recommended technologies for providing privacy in instant messaging

2.1. Research strategy choice

This research will mainly rely on the case study as the main methodology, as it allows a detailed analysis of the consequences of the use of new technologies and their impact on improving security in applications.
Case study is a general term, the so-called examination of a particular event or situation, as well as a useful type of observational research. It is a common method for analyzing malware, threats or the implementation of new policies and procedures. One of the strengths of case studies is that they involve a variety of sources of evidence - documents, artefacts, interviews, observations [4]. The presented study relied on software documentation and interviews with cybersecurity experts.
Although individual assessments and studies of cyber system behaviour may not be general, they will contribute to a systematic set of knowledge.
Thus, case studies of the implementation of personal data security technologies in the most popular instant messaging applications were conducted and recommendations were made for further composite usage of certain technologies to develop a more secure application than existing ones on the market.

2.2. Encryption

In IM, the following encryption methods are mainly used:

1. End-to-end encryption (E2EE) protects the message transmitted from sender to recipient and ensures that the information is converted into a secret message by its original sender and decoded only by the last recipient. No one, including the application you use, can listen to or access your activity. This is the main characteristic of good encryption: even people who develop and deploy it cannot break it themselves [5]. If we are sure that we are using E2E encryption correctly, the server will never be able to read our message.
2. Signal encryption algorithms. Even though several measures have been taken in end-to-end encryption for instant messaging, the most significant breakthrough in this area has been the Signal messaging protocol, "a secret data distribution protocol operating in synchronous and asynchronous messaging environments." Signal's goals include end-to-end encryption, as well as advanced security features such as perfect direct secrecy and forward secrecy.
The Signal Protocol amalgamates the Extended Triple Diffie-Hellman (X3DH) key agreement protocol, Double Ratchet algorithm, pre-keys, and uses Curve25519, AES-256, and HMAC-SHA256 as cryptographic primitives.
Next we will describe each of the algorithms, their meanings and principles of operation.
– *X3DH*. It starts by generating all the necessary keys between the two parties for communication and establishes a common secret key between the two parties, which mutually authenticate themselves based on their public key pairs. The X3DH also allows keys to be exchanged when one party is offline, and will be exchanged through a third-party server instead [6].
Although the protocol has a long history, the security of the protocol has only recently been proven, by demonstrating a scenario in which a powerful adversary controlling the network cannot rely on a shared secret key to expose messages sent. This is also true for a situation where the adversary has access to some secret values that are used to calculate the shared secret key.
– *Double Ratchet Algorithm*. The double ratchet algorithm is used as part of a cryptographic protocol to provide E2EE based on a shared secret key derived from X3DH. Once both parties agree on a shared secret key through the X3DH, they can use the Double Ratchet to send and receive encrypted messages.
The key derivation function (hereinafter - KDF) is the basic concept of the Double Ratchet algorithm. KDF is defined as a cryptographic function that takes the secret and random KDF key and some input and returns the output. The initial data cannot be distinguished from the random, provided that the key is unknown (i.e. KDF satisfies the conditions of the pseudo-random function, the construction of which is dealt with by many scientists, in particular [7]). If the key is not secret and random, KDF must still provide a secure cryptographic hash of its key and input.

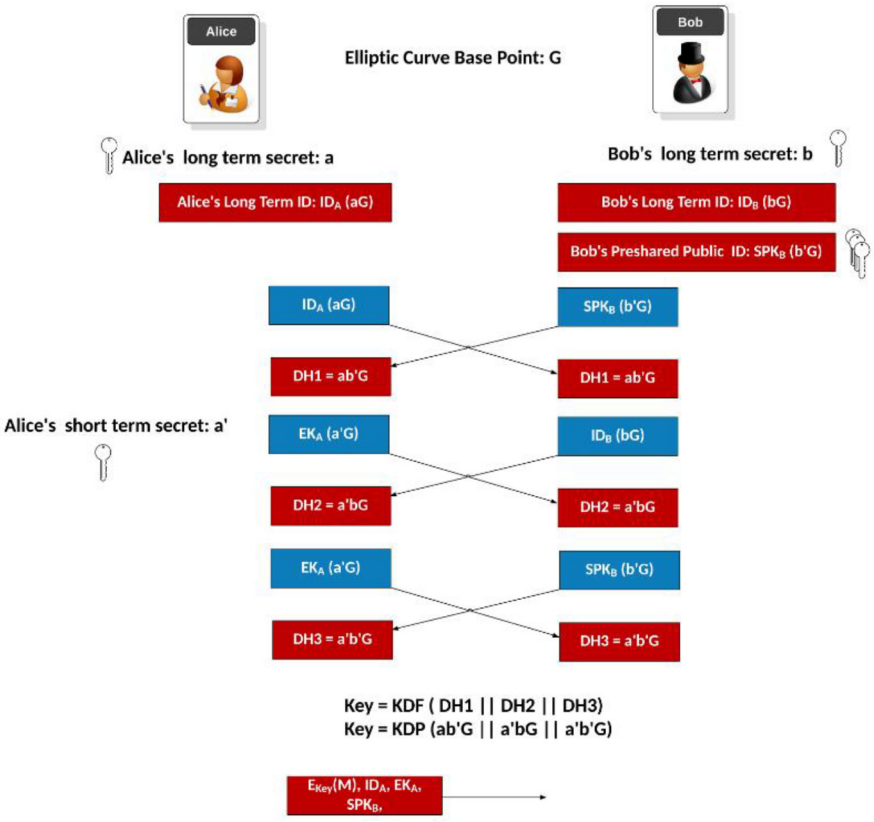

Figure 2. X3DH operation principle

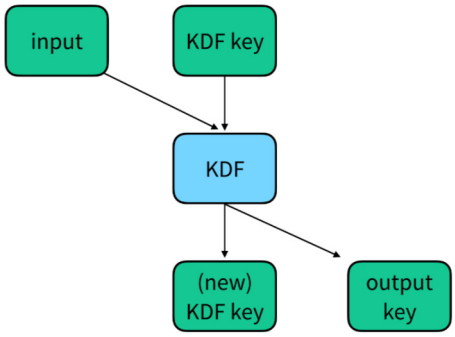

Figure 3. KDF chain step

The developers refer to the algorithm as self-healing because it automatically disables an attacker from accessing the cleartext of later messages after having compromised a session key. The protocol provides confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, backward secrecy

(aka future secrecy), causality preservation, message unlinkability, message repudiation, participation repudiation, and asynchronicity.
– *Curve25519*. Curve25519 is an elliptic curve and a set of parameters selected to it in such a way as to provide higher performance (on average 20-25%) and get rid of some safety problems in the traditional elliptical Diffie-Hellman curve (ECDH).
The principle of operation is shown in fig. 4. This algorithm has been carefully designed to allow all 32-byte strings as Diffie-Hellman public keys. The Signal protocol uses Curve25519 for all asymmetric cryptographic operations.

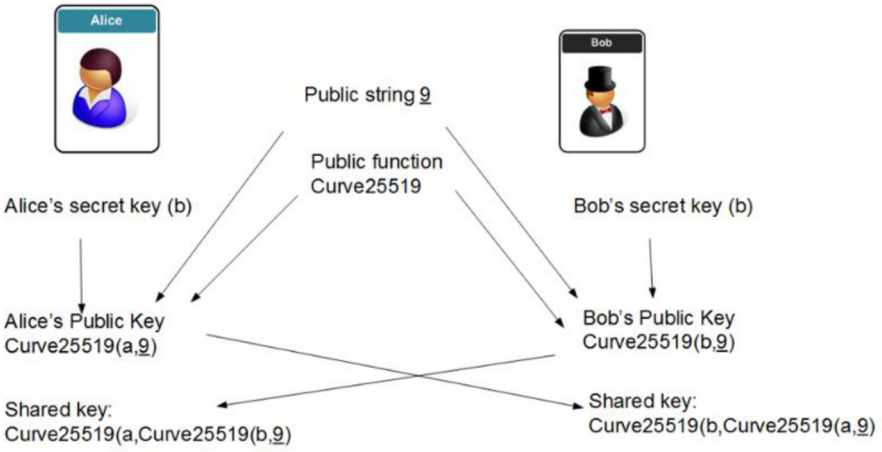

Figure 4. Curve25519 method

The scheme differs by its simplicity and speed. In addition, it is resistant to time attacks, i.e. attacks by a third-party channel in which the attacker threatens the cryptosystem, analyzing the time required to perform cryptographic algorithms.

2.3. Voice and video calls protection

Because video calls and voice messages contain personal information in its purest form, they are particularly in need of protection. Video and voice protection solutions are researched in the Threema case study.
Threema calls are based on WebRTC, an open IETF standard. WebRTC uses the ICE, STUN and TURN protocols to establish a secure peer-to-peer connection [8]. All connections are secure and encrypted with DTLS (Transport Layer Datagram Datagram) and SRTP (Real-Time Data Protocol).
WebRTC is an open-source voice or video chat system that uses two types of servers for signalling and media transmission, which ultimately allows devices on a separate LAN to find and interact with each other. WebRTC requires alarm, STUN and TURN functions.
The Threema implementation encrypts video calls between users' devices using locally stored encryption keys. This prevents "middle man" attacks, in which attackers may want to intercept calls.
All E2EE video calls are established between users in such a way that the traffic flows between them directly without passing through Threema servers. The only exception

for which Threema servers are involved in calls is when users start a call with an unverified user.
In addition, the new video call feature not only encrypts the video stream itself, but also its metadata; a decision that prohibits network observers from displaying any details about a video call.

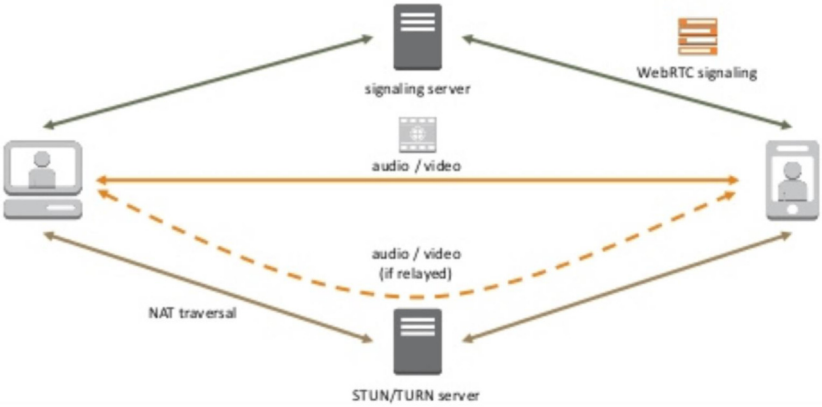

Figure 5. WebRTC operation principle

2.4. Anonimity

Most popular messaging programs require the user to register via email or phone number to be able to use the service. This provides some benefits, including checking your account to protect against spam and detect social networks. However, such requirements also create significant privacy and security concerns for users.
Using a phone number as the basis for owning an identification key/long-term key pair weakens the protection against compromising user accounts, for example in the case of popular programs such as Signal and WhatsApp. This weakness is primarily related to the fact that telephone numbers are managed by centralized service providers, which can bypass the control of users, allowing these providers to directly control specific user numbers. In addition, techniques such as SIM swap scam attacks, service provider hacking, and phone number processing can be used by lower-level scammers. In most countries, users are also required to provide personal information, such as a passport, driver's license or identity card, to obtain a telephone number that will be permanently linked to their personal data. These credentials are stored in private databases that can be accessed by the many web scrapers and indexers that automatically collect phone numbers associated with specific individuals. Phone number-based account systems also limit the ability to set multiple credentials by a single user.
The use of email addresses is also a reasonable threat to user anonymity. In case of getting access to the user's mailbox, the attacker can impersonate, crack passwords to accounts, collect personal information and steal identity.
Instead of email addresses and phone numbers, Session Messenger uses Session ID as the basis for creating an account. Session ID is a pseudo-random alphanumeric sequence that serves as an account ID and looks like this:
05067a2e9896678aa966ed3ece82d12f28344d4e669db98f6f2183411a8c98797c.

Session IDs do not need to be associated with other identifiers. It acts as a pseudonym and provides absolute anonymity if the user does not associate it with the individual by external actions.
Because Session does not have a central server for maintaining user credentials, the generally expected user experience of being able to recover an account using a username and password is not possible. Instead, users are encouraged to write down their long-term private key (recovery phrase) after creating an account. The user can use this backup key to restore their account if their device is lost or destroyed and the user's contacts can continue to contact the same account instead of re-initiating contact with the new key.

2.5. Data storage

Despite the convenience of storing messages and data on devices or even in cloud storage, as implemented in Telegram, this approach is not safe. In this case, the developer will always have access to user data, as well as anyone who will have access to devices with the application installed will be able to read the message.
The safest approach is automatically deleting messages and attachments, which will be analyzed on the example of Wickr.
Wickr uses patented burn-on-read technology, which automatically deletes all messages and any attachments upon receipt, based on user settings. Individual users or network administrators can configure Wickr automatic destruction settings to set the exact interval after receipt when messages and attachments are securely deleted. All messages are securely shredded, and no messages are stored on sending or receiving devices or servers.
Wickr uses "Expiration" and "Burn-on-read" timers:
- "Expiration" sets the empirical maximum amount of time during which the content can live; it starts counting down the time when the message is sent.
- "Burn-on-read" automatically deletes a message once it has been read by its recipient; it starts counting down as soon as the content is marked as "read", but never extends the life of the content beyond the time of destruction defined by the value "Expiration".
In addition to reducing the risk of recovering deleted Wickr data, Secure Shredder is launched whenever Wickr is running. The goal is to "disinfect" or overwrite deleted Wickr data. Secure Shredder clears RAM after each opening of a message or attachment.

2.6. Password protection

All of the aforementioned technologies, even combined, will not protect against someone accessing an unlocked device, so it's worth mentioning the password protection of the instant messaging application.
For example, the Wire application offers the App-lock function, which requires authentication with a password or biometrics (depending on the user's choice) each time the application is launched. You can also specify the time after which the application will be blocked.
To increase security, the password cannot be recovered if the user has forgotten it. The user will be forced to sign out and the message history will be deleted.
This approach protects against unauthorized access in the following situations:

- The third-party accesses the device with the application with or without the consent of the owner;
- The device is left unattended with the application open.

3. Conclusions

Improving the effectiveness of the protection of personal information in instant messaging services is an extremely important task that requires constant attention. The tendencies of solutions for ensuring the protection of personal information have been demonstrated: anonymization, decentralization, privacy management and configuration, encryption, and providing information, legislation and rules. Based on case studies of instant messaging applications such as Signal, Session, Threema, Wickr, Wire, the most effective approaches to ensure the protection of users' personal information have been proposed. It is proved that the implementation of the selected technologies practically eliminates the possibility of realization of certain threats. Using the proposed approaches, a more secure instant messaging application can be further developed than currently available.

REFERENCES

1. CURRY SAMUEL J.J.: Computer and Information Security Handbook, third edition.
2. Secure Messaging Apps Comparison: *https://www.securemessagingapps.com*/.
3. KLEPPMANN M.: The Investigatory Powers Bill would increase cybercrime: *https://martin.kleppmann.com/2015/11/10/investigatory-powers-bill.html.*
4. YIN R. K.: Case study research: design and methods. Fifth edition, 2014
5. Surveillance Self-defence: https://ssd.eff.org/en/glossary/end-end-encryption.
6. Signal. The X3DH Key Agreement Protocol: *https://signal.org/docs/specifications/x3dh*/.
7. GARASIMCHUK O.I., MAKSYMOVYCH V.N., MANDRONA M.N., KOSTIV Y.M.: A Study of the Characteristics of the Fibonacci Modified Additive Generator with a Delay, Journal of Automation and Information Sciences, DOI: 10.1615/JAutomatInfScien.v48.i11.70 pages 76-82.
8. HMAC: Keyed-Hashing for Message Authentication: *https://datatracker.ietf.org/doc/html/rfc2104*.