Instant messaging security and privacy secure instant messenger design

R M Ali¹, S N Alsaad¹
¹Department of Computer Science, College of Sciences, Mustansiryah University, Baghdad, Iraq

Abstract. Among many types of social network applications, instant messaging is one of the applications that consider the privacy and the security are two crucial features due to that data exchanged between users are often private and not for public. In this work, a secure Instant Messenger (IM) mobile application is designed and implemented. Many techniques are used to provide privacy and another to achieve security through suitable cryptographic method. The limited and varied specifications of users' mobile devices are considered for implementing the concept of end-to-end encryption. The application also providing the main functions of instant messaging applications such as profile creation, access control management, and finding friend.

1. Introduction

In the last years, Online Social Networks (OSNs) have become the most preferable and convenient means of communication between people. These networks offer an easy and inexpensive way to continuance existing relationships and forming new ones by providing an attractive means for sharing information and digital social interactions especially those that are by mobile phones such as Instant Messaging (IMs).

The rapid development of social networks and the widening of their popularity makes them vulnerable to security and privacy risks and suitable channels to attracts hackers and intruders [1] [2]. In existing OSNs especially Instant messengers IMs, there are several privacy and security problems that need to be resolved, and protect user personal information and shared data over these messaging applications [3].

The most important related work in this topic was used as references for this paper such as in [5] the researchers suggested approach deal with security and privacy problem in OSNs in order to assure privacy of users against the privacy violations by the service provider based on tow principles, Decentralization, and exploiting of real life trust. In addition, other researchers in [3] present analysis of Telegram Messenger and the related MTProto Protocol with cryptography behind Telegram and with a description of current security status for some major instant messengers. Meanwhile, researchers in [6] discussed types of threats on privacy of social networks and ranges of its effects as user related and provider related. While, in the paper of presented in [4] the researchers discussed social network security and trustworthiness as a new trend in the research of security of social networks and awareness of users.

In this work, the threats on the privacy of social networks and the trends of its solution were described, then the criteria of security in IMs are depicted to be standard to evaluating of IM application, and the last main section is the design of proposed secure IM application.
2. The most serious threats
The most serious threats to the privacy and security of social network users are those of untrustworthy network service providers because all user data in the system is within their reach. The analysis of security and trustworthiness still lacks sufficient and at the same time the present security and privacy challenges increasing. It is very necessary to find realistic solutions for increase the trustworthiness and security [4]. It is noticed that majority of OSNs users of social networks do not have sufficient awareness of the risks of security and privacy which needs to be taken into account when designing solutions to the threats suffered by those networks.

In addition to the inside attackers, that seem to legitimate participants but act in a malicious way, there may be external attackers, or intruders, who can launching attacks on one or more of Social Network Services (SNS) levels which can be divided into three categories: Social Network SN, Application Services AS, and Communication & Transport CT level. According to this architecture there is an attacker can be defined as one of, malicious user on SN level, malicious provider on AS level, party that has access to the CT level infrastructure [5].

3. The trends of solutions
It is important to review the solutions contained in the current researches in this area to address these problems, reduce their effects, mitigate privacy issues, and meet the privacy needs of users of OSNs. In such field there are many trends can be distinguished:

3.1 Anonymization
Simply it eliminates all identifying or identifiable information from the data to be hidden from the OSN [6]. When the service providers share their data for the research purposes, very sensitive users information could appear implicitly or explicitly from the social graph, so there should be an anonymized way that reduces the probable risks for their users [7]. However, the drawback of this trend is that it is hard to prove these methods to be secure, compared to traditional cryptographic operations.

3.2 Decentralization
Users' data privacy in OSN is at risk due to the central management and storage and actually malicious providers threatened or unpremeditated access following publication. Which cannot be assured with server-based centralized architectures. As a suitable substitute for the centralized approach, the Peer-to-peer architectures provided the basis for a decentralized OSN in the way of avoiding the all-knowing service provider [5]. The drawback is a lack of a priori trust, which need to cooperation and exploit on real life trust between users, but the biggest problem may be lied in the technical feasibility of a fully decentralized OSN, because of Providing data availability and integrity and updating management is very hard in this setting.

3.3 Privacy Settings and Management
Most users of OSNs are not wary or careful about privacy settings of their profile, although most OSNs provide settings to manage privacy for the users to control what information they want to share and whom people they want to connect. However most users don't have full awareness about the information they have explicitly or implicitly disclosed and mostly accept the provided default privacy settings, and may be disclosed the more sensitive information which represent the highest risk level for the user privacy. The research in this field revolves around increasing users control over their privacy settings, or make it easier, it hopes to mitigate the risk of unauthorized access and the user inability to hide sensitive information from a specific participants such as friend or group [6]. In the field, it is very important to enhance users' awareness of privacy by showing them the consequences of their actions.
3.4 Encryption
Used as a tool to provide confidentiality aspects and as the basis for integrity. According to how encryption is applied, the encryption can be effective in protection from unauthorized users or the service provider. It is also used as a building block combined with other proposals trend, such as privacy settings and management tools or decentralization systems [8]. The encryption is very necessary in order to hide user information from the OSN, while using central infrastructure.

3.5 Awareness, law and Regulations
Non–Technical research focuses on the improvement of awareness of users for privacy issues in OSNs, and compliance of both service providers and users to social conducts and established laws. Most of these non-technical approaches without actively enforce the changes proposed. On the other side, the Policies and regulations related to privacy are not mandatory, and awareness is usually needed time to be raised, laws solve problems after things go wrong, while technical solutions used to prevent violations [8].

4. The Instant Messaging (IM) & Security Aspects
Today, most social networks provide some form of real-time online messaging, the users are very demanding. IMs are required to have both mobile and web access with more advanced capabilities, such as media, voice, or location sharing, and ability to see if a contact is online and available for a chat [3].

Because of the nature of these applications and the more private nature data exchanged between users in terms of the vast amount of data and in terms of inappropriate for publication to the public as in other types of social networks, hence the topics of security and privacy are important in the evaluation of IM Applications.

The Electronic Frontier Foundation EFF maintains a scoreboard of messaging applications' security, it evaluates messengers (tested 40 messaging applications) based on the following criteria: [9]

- Is the message encrypted in transit? User communication must be encrypted. (metadata, like usernames, phone numbers, or dates, is not required to encrypt).
- Is the message encrypted in such a way cannot be accessed by the provider? End-To-End encrypted, from the moment message sends by the user to the moment it received by the other party. No re-encrypting or decrypting may occur during that process, only the two parties of communication should be able to decrypt messages. The private keys have to be generated at the endpoints, not at a centralized server.
- Can the user verify contacts' identities? A verification mechanism requires to opposite side's identity to prevent Man-in-the-Middle attacks.
- If the keys are stolen, are the past communications secure? The messages must be encrypted with routinely changing keys. This requires end-to-end encryption as in the second criterion.
- Is the code open to an independent review? The Source code be released as a free/open source license, but to pass only requires releasing the code that affects the encryption and communication performed by the client application.
- Is the cryptography design well documented? The cryptography behind the messaging application and its explaining should be placed on record in the detailed documentation, and can answer the following, which algorithms and parameters (such as key sizes) are used, how keys are generated, and how exchanged between the users and the keys life-cycle and the process for users to revoke or change their key.
- Has there been an independent security audit? A security review of the messenger application must not be older than 12 months. It is not required that the audit is available publicly [9].

5. Proposed Secure IM
The proposed application is an attempt to find useful solutions to the problems of security and privacy in the field of social networks.
The major structure of the proposed system is depicted in figure 1. The system is developed as a mobile application using JAVA & XML languages under Android Studio environment, MySQL database, SQLite local database, and Node.js (Java Script) platform for server programming, C Sharp language is adopted for interface designing. All messages exchange over this proposed IM (Texts, Images, and Files) are end-to-end encryption using lightweight algorithms for encryption and decryption to be convenient for limitation and diversity of user mobile devices. The design includes three main levels described as parts as follows:

**Part 1: Basic Functionalities of IM**
The proposed application provides the major functionality required for the IM. The application design needs to build two types of databases, the main system database on the server which holds user information, status, friends and messages exchanged of all users in the system, while the Local database which is built inside the user device to hold the user information, Conversations, and some important status. These two databases are designed to store and manipulate three types of messages (text, images, and files) as either encrypted or unencrypted form in accordance with sending or receiving messages status. The Basic tasks are presented follows:

**Registration and Log in:** Once the user opens the application, a set of processes will be performed to check local and global (server) databases if this phone number is already registered to facilitate user log in and opening the list of chat friends interface, otherwise, new registration process is implemented to get phone number of new participant and send verification SMS for identity authentication.

**Checking Processes:** The application adopts some of checking processes like:

- **Level of the user:** Two types of users are considered (VIP and normal) specified by the admin. In the VIP level, additional security, privacy features and some additional procedures related to security and
privacy are added. **New Friends:** If any new friend (contacts) of the user is registered as a new member in the application, the list of friends of this user will be updated. The application makes checking for all user contacts in every log in.

**New Messages:** When a new message arrived (upload) to server and receiver status is online, all new messages will be downloaded from the server database to local database inside user (receiver) device with notifications of new unread messages.

**Access Control Management:** To make sure the user registering in the system is a real person and not a robot or a compromised user account, and for avoiding Identity Theft or Profile Cloning. The main Authentication Mechanisms are adopted:

a. *Verification message (SMS):* During registering in the application by the user's phone number, the server sends a verification message (SMS) containing a random code to be used as verification the registration for this phone number. This mechanism can be applying repeatedly and automatically as needed according to user level. This mechanism required to take user permission to access his/her mobile SMS.

b. *ICCID Checking:* For every mobile SIM card there is a unique non-recurring code number called ICCID (Integrated Circuit Card Identifier). The proposed application used ICCID to make sure that the registered phone number is the same SIM card number for the device that connects to the application, to detect any unauthorized attempt to access by user number from a device that does not have the SIM card of this user registered phone number.

**Part 2: Privacy Techniques**

This part is to overview the privacy techniques and features that used to reinforcement the security and privacy aspects in the proposed application accompaniment to the problems of user awareness, these techniques are:

- **Messages Dealing:** This technique is used to allow just for stored contacts on the user mobile phone device to messaging with the user via this application. When a message arrives from someone who is not stored under user contacts, it will appear at the recipient notification to have the option of accept the messaging from this sender or not.

- **Contact Blocking:** The proposed application gives the user the right to block any contacts whom the user does not want to communicate, at the same time, the user can unblock as well. This technique is used as a form of privacy protection.

- **Session Destruction:** An optional choice allows the user to destroy the conversation. This means that all conversation data and messages will be erased from the local and global databases and cannot be retrieved.

**Part 3: Cryptographic Techniques**

One of the major problems that the proposed IM application faced is how to make the user's private information and exchange data (messages) between them are more secure, so that the message encrypted in such a way cannot be accessed by the provider. This is called End-To-End encryption which is mean that the message encrypted on the sender device, only the receiver can be decrypted it.

The general structure of the cryptographic techniques of the proposed system is depicted in figure 2. It consists of two parts. The first part concerns with key management between the sender and receiver, while the second part concerns encryption and decryption chatting messages. The idea of using RSA algorithm is to ensure the secret key (for Trivium algorithm) is protected and transferred between sender and receiver safety. The flow events of key management part are:

1. The sender encrypts the secret key by the public key of the receiver.
2. The receiver decrypts the encrypted secret key using his private key of RSA algorithm.
3. The receiver used the decrypted key to decrypt the message using Trivium algorithm.

The second part exploits Trivium stream cipher to encrypt the chatting messages between the sender and receiver using secret random key (96-bits) which is combined with most significant bits (64-bits) of UUID function (Universally Unique Identifiers) for a receiver phone number to create a 160-bits as
main input of Trivium algorithm. UUID is time-based generated identification mechanism [10].

1-Message Encryption
In the proposed application, the messages exchanged between users are end-to-end encryption that means the encryption process will be done on the sender device and the messages are transmitted from sender to receiver through server and stored in the main database in encrypted form, while the decrypted process will be done on the receiver device.

Before message encryption, a pre-processing is required for configuring 160- bits for phase 1 of Trivium algorithm. These 160 bits consisted of 64-bits from the function of UUID most significant bits (for receiver number) and 96-bits from secret key which is generated randomly, 160-bits divided into two halves 80-bits for key and 80-bits for Internal Value (IV). These two inputs will produce 288-bits as state Register after a lot of shifting and rotate iterations as an output for the phase1 of Trivium algorithm [11], which is beginning with the event of selection of user to one of contacts from friend list to start chatting. All these processes (Trivium phase1) are performed for one time in every session between two users.

Phase2 will be beginning with the first message is sent and repeated with every next message during the same session. The output of phase1 (288-bits State register) is an input of phase2, and the final output is produced N-bits Key stream, where N is length of the message (N<264) generated by several shifting and rotate operations similar these operations in phase1 [12].

The generated Key Stream will be XORed with message bits to produce an Encrypted message, which is uploaded to the application server to be sent to the receiver.

![Diagram](image.png)

**Figure 2.** General structure of the cryptographic system of proposed application.
All messages exchanged via the proposed application and stored in the server database are encrypted. For every sending message there is a secret key used in the encryption process at the sender. To decrypt the messages, this key must be transmitted to the recipient in an encrypted format so, we need an asymmetric encryption algorithm (e.g. RSA) to encrypt the secret key along with the message encryption. Asymmetric algorithm RSA uses the public key to encrypt secret key at the sender while it uses the private key to decrypt at the receiver who owns his private key exclusively [13]. Figure 3 shows these processes.

2-Message Decryption
The private key of the receiver will be used via RSA to decrypt the encrypted secret key which is used to decrypt the sender message via Trivium in a manner similar to the Trivium two phases in encryption stage. Figure 5 shows general decryption processes for the secret key and the message received at the receiver side.

Beside the security concept, the speed of Messaging is an important criterion in the IM applications. Therefore, it is necessary to increase the efficiency of Trivium algorithm from side of reducing encryption and decryption time. This can be achieved through some of modifications as following:

1. Separate the two phases of Trivium and running phase 1 for one time per session start with event of select friend from list of friends to chat beginning, even before the first message sending, this phase generate 288-bits state register, while phase 2 repeated with every message sending, to generate key stream and XORed with bits of the message.
2. Minimized the iterations of (For) loop in phase 1 as less as possible (288 loops).
3. In case of very long message length (e.g. large size image) it may be divided the key stream of one message into sub key streams each one equal to long of bits for the part of the message (section of image pixels).

These modifications have increased the efficiency of encryption and decryption on the sender and receiver by more than 40%.
**Figure 3.** Message encryption flowchart

Three types of messages in the proposed application are encrypted in the sender and decrypted in the receiver (text, image, and file). Figure 4 offers an example of image encryption in this method.

**Figure 4.** Example of image encryption
Figure 5. Message decryption flowchart

After the implementation of this IM application in the real environment, the evaluation of main tasks, privacy techniques, and cryptographic methods, which are used in the proposed application design, gives an accepted output for both security vector and performance (speed) vector as balanced results. So that all the standard EFF criteria of IM security are satisfied as described in the following table:

Table 1. Satisfaction all the standard EFF criteria of IM security

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

8. Conclusion

The most users of OSNs are generally not conscious to the importance of privacy settings to secure their personal information, so they do not have enough awareness to realize the risk of several threats that facing their privacy, so that it is necessary to make some of the necessary protection features automatically managed by the application. Furthermore, the most serious threats to the security and privacy of social media are those of untrustworthy network service providers because all user data is within their reach. In addition to that, the used of end-to-end encryption concept and key exchange techniques are the main vectors in the privacy and security analysis and evaluating of social networks.

References

[1] Ebinezer M and Suresh B. 2015 Security Strategies for Online Social Networks International Journal of Computer Trends and Technology (IJCTT) 5(5)
[2] Abdullah S M 2017 A Multi Secret Sharing Approach for Vulnerability Identification in Social Media The 1st International Conference on Information Technology (ICOIT’17) p.45
[3] Sušánka T 2017 Security Analysis of the Telegram IM Master’s Thesis, Czech Technical University.
[4] Zhang Z and Gupt B B 2016 Social media security and trustworthiness: Overview and new direction Future Generation Computer Systems 86 pp.914-925.
[5] Cutillo L A 2007 A Privacy Preserving Online Social Network Leveraging on Real-Life Trust IEEE Communications Magazine 47(12) pp.94-101
[6] Beye M, Jeckmans, A J, Erkin Z, Hartel P, Lagendijk R L, and Tang, Q 2012 Privacy in online social networks. In Computational Social Networks pp. 87-113
[7] Boshrooyeh S T, Kupc A and Ozkasap O 2015 Security and Privacy of Distributed Online Social Networks in International Conference on Distributed Computing Systems pp.112-115.
[8] Abraham A 2012 Computational Social Networks Security and Privacy in Springer Science & Business Media ISBN 978-1-4471-4051-1,
[9] EFF Security aspects of messaging website: https://www.eff.org/pages/secure-messaging-scorecard. Accessed 25-1-2020
[10] Balkić Z, Šoštarić D and Horvat G 2012 GeoHash and UUID Identifier for Multi-Agent Systems KES-AMSTA, LNAI 7327 pp. 290–298.

[11] Diedrich L, Jattke P, Murati1 L, Senker M and Wiesmaier A 2016 Comparison of Lightweight Stream Ciphers:MICKEY 2.0, WG-8, Grain and Trivium”

[12] Christophe de Cannière, Bart Preneel, 2006 Trivium Specifications” eSTREAM, ECRYPT Stream Cipher Project

[13] Stallings W 2006 Cryptography and network security, 4/E. Pearson Education India.