Developing an End-to-End Secure Chat Application

Article · November 2017

CITATIONS
0

READS
1,239

3 authors, including:

Noor Sabah
Al-Nahrain University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Ban N. Dhannoon
Al-Nahrain University
41 PUBLICATIONS **42** CITATIONS
SEE PROFILE

Developing an End-to-End Secure Chat Application

Noor Sabah, Jamal M. Kadhim and Ban N. Dhannoon

Department of Computer Science, Al-Nahrain University, Baghdad, Iraq

Summary
Chat applications have become one of the most important and popular applications on smartphones. It has the capability of exchange text messages, images and files which it cost free for the users to communicate with each other. All messages must be protected. The aim of the paper is to propose chat application that provides End-to-End security that let safely exchange private information with each other without worrying about data. In addition to the protection of storage. A list of requirements to make secure chat application is presented in this paper and based on these requirements, the application was designed. The proposed chat application was compared with other popular applications based on those requirements as well as it has been tested as a proof for providing End-to-End security.

Key words:
Secure chat application, Security, Android, Secure session, Secure storage

1. Introduction

With the rapid development of mobile phones, mobile devices have become one of the integral part of daily activities. In recent years, chat applications have evolved and made a major change in social media because of their distinctive features that attract audiences[1]. It provides real-time messaging and offers different services including, exchange text messages, images, files and etc. Moreover, it supports cross platforms such as Android and iOS. There are currently hundred millions of users smartphone are using chat applications on monthly basis[2].

There are two types of architecture in those applications, client-server and peer-to-peer networks. In a peer-to-peer network, there is no central server and each user has his/her own data storage. On the contrary, there are dedicated servers and clients in a client-server network and the data is stored on a central server[3].

Security and privacy in chat applications have a paramount importance but few people take it seriously. In a test done by the Electronic Frontier Foundation, most of the popular messaging applications failed to meet most security standards. These applications might be using the conversations as an information for certain purposes. Moreover, reading the private conversations is certainly unacceptable in terms of privacy.

Most applications only used Transport Layer Security (TLS) for securing channel, the service provider has full access to every message exchanged through their infrastructure [4]. Therefore, these messages can be accessed by attackers. Therefore to maintain protection and privacy, messages should be encrypted from sender to receiver and no one can read messages even the service provider, in addition to protecting the local storage of the device [5].

In this paper, we focus on security, privacy and speed by proposing end-to-end security which ensures only sender and receiver can read messages without a third party. As well as storage protection and fast transfer of messages between the parties.

The main contributions of this paper are the following:

1- Propose client-server mobile chat application which supports the status of the communicating parties whether online or offline.
2- Provide a friendship request service.
3. Secure key exchange, then calculate the session key.
4. Secure exchange of end-to-end messages.
5. Analysis and Test the proposed chat.

2. Mobile Chat Applications

In this section, we briefly introduce many of popular chat applications in the mobile market according to security and privacy concerns. Unfortunately, some chat applications are not public or open source makes it difficult for evaluated by the developer's community, security experts or researcher academic.

2.1 Viber

Viber is an instant messaging and Voice over IP (VoIP) application for smartphones developed by Viber Media. In addition to instant messaging, users can exchange images, video and audio media messages. Viber recently supported the end-to-end encryption to their service, but only for one-to-one and group conversations in which all participants are using the latest Viber version 6.0 for Android, iOS or Windows 10. At this time, in the Viber iOS application for iPhone and iPad, attachments such as images and videos which are sent via the iOS Share Extension does not support end-to-end encryption [6]. Viber has privacy issues such as adding a friend without his knowledge or adding him to a group without his permission. Plus that, local storage is not secured. It is not open source making it difficult to evaluation.

Manuscript received November 5, 2017
Manuscript revised November 20, 2017

2.2 WhatsApp

WhatsApp is one of the most popular messaging application, recently enabled end-to-end encryption for its 1 billion users across all platforms. WhatsApp uses part of a security protocol developed by Open Whisper System, so provides a security-verification code that can share with a contact to ensure that the conversation is encrypted [7]. It is difficult to trust in WhatsApp application completely because the application is not open source, making it difficult to verify the functioning process and match them with the work of the encryption protocol which was announced.

2.3 Telegram

Telegram is an open source instant messaging service enables users to send messages, photos, videos, stickers and files [8]. Telegram provides two modes of messaging is regular chat and secret chat. Regular chat is client-server based on cloud-based messaging, it does not provide end-to-end encryption, stores all messages on its servers and synchronizes with all user devices [9]. More, local storage is not encrypted by default. Secret chat is client-client provides end-to-end encryption. Contrary to regular chat messages, messages that are sent in a secret chat can only be accessed on the device that has been initiated a secret chat and the device that has been accepted a secret chat they cannot be accessed on other devices. Messages sent within secret chats can be deleted at any time and can optionally self-destruct [8].
Telegram uses its own cryptographic protocol MTProto, and has been criticized by a significant part of the cryptographic community about its security[9].
The registration process of Telegram, Viber and WhatsApp depend on SMS. SMS is transported via Signaling System 7 (SS7) protocol. The vulnerability lies in SS7 [10]. Attackers exploited SS7 protocol to login into victim's account by intercepting SMS messages [11]. Because of Telegram cloud-based, the attacker exploits it and makes full control of the victim account and can prevent him to enter into his account. To make the account more secure should activate two-factor authentication [12].

2.4 Facebook Messenger

Facebook Messenger is a popular messaging service available for Android and iOS. It provides two modes of messaging is regular chat and secret conversations. Regular chat does not provide end-to-end encryption only secure communication by using TLS, and it stores all messages on its servers. Secret conversations have the same idea of Telegram secret chat [13].

3. Proposed architecture

3.1 Secure Mobile Chat Requirements

In this section, we propose a set of requirements to make secure chat application:
req1: Password stored on the chat server should be encrypted.
req2: Providing either secure session or TLS. Secure session is a unique key for each session. Ensures that communication is with the right person and no man-in-the-middle can read the messages.
req3: Messages must be encrypted to maintain security and privacy.
req4: Local storage must be protected by encryption.
req5: Messages are not stored on the chat server but stored on the user's device.
req6: It is not allowed to exchange messages if they are not friends.

3.2 Proposed Architecture

The proposed architecture is designed to be Client-Server chat application. In client side, when a user sets up the application, the user either selects registration or log-in. In server side, the chat server consists of users' server and a message server. User's server that manages user's credentials. Message server handles messages between users by using Firebase Cloud Messaging (FCM).If the recipient is offline, the messages will be stored temporarily on the FCM queue for a specific period of time, and when recipient becomes online these messages are forwarded to him then deleted from the queue. The generic architecture is shown in Fig. 1

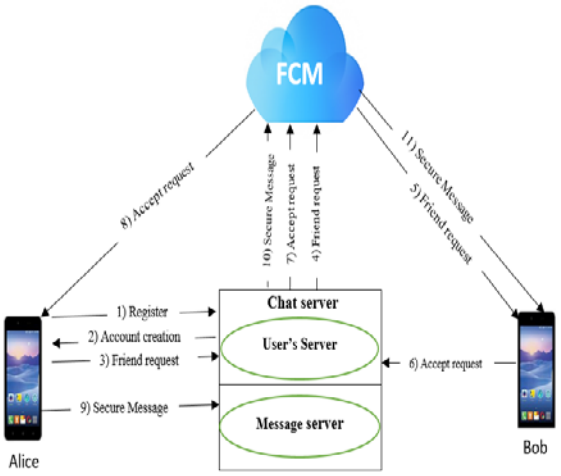

Fig. 1. Generic Architecture of Proposed Chat.

3.3 Registration an account

Before starting the application, there must have a lock screen to configure the Keystore that provides a secure container to store the local storage key to make more difficult for extraction it from the device by unauthorized persons or other applications [14].
Each account has only one device and it is distinguished by device id. In addition, Email and username are unique.
Name, email and password are required to register a new account. After typing the registration information, the password is encrypted by using XSalsa20 algorithm [15]then the user credentials are sent to the server. After verification, the server generates a unique identifier that acts as the user ID. After that, the acknowledgement message is received for successful registration to the client application and the client information is stored in local storage.
The application generates a set of keys:
(a) Key for encrypting the password.
(b) A public key pair for calculating session key.
(c) Symmetric storage key for encrypting/decrypting local storage contains contact list, chat history and key store.

3.4 Login

Email and password are required for user authentication. After typing the authentication information, the password is encrypted then the user credentials are sent to the server. The server checks if the email and password are valid. After validation, JSON Web Token (JWT)[16] is created and sends to the client to store it. When a client makes a request at the later time, JWT is passed with the request. The server verifies of the JWT, if it is valid, the request is processed (Fig.2).

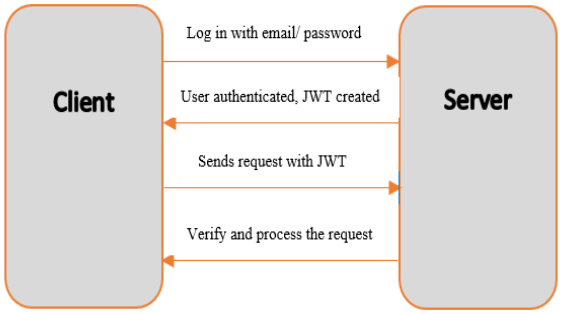

Fig. 2 Login process.

3.5 Firebase Cloud Messaging

Firebase Cloud Messaging (FCM) is a service that facilitates messaging between mobile applications and server applications. It's built on Google Play Services that supports cross-platform (iOS, Android & Web). It is a free service that allows sending lightweight messages from the server to the devices whenever there is new data available[17]. This saves a lot of user's battery by avoiding requesting to the server for new messages. It provides TLS for securing channel.
At the beginning of running the application for the first time gets the following:
(1) The application connects to FCM server and registers itself.
(2) When successful registration, FCM provides registration token to the device. This registration token uniquely identifies each device.
(3) The application sends the registration token to the server to store it in MongoDB database.
The above steps are shown in Fig. 3.

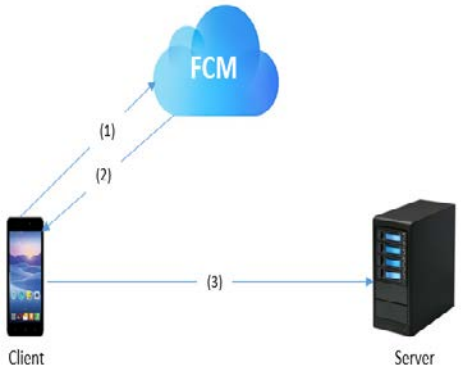

Fig. 3. Firebase Cloud Messaging.

When the server sends a push notification, it sends a request to FCM sending the push message along with the registration token. FCM identifies the target device by using registration token then starts to push data.

3.6 Session key Setup

To add users to contact list either by username or by email address.
For sending a request to a friend on the assumption that the first user knows the username or email of the second user due to the username and email are a unique for each user and the second user should have already registered in the server. Presumably, the first user is called Alice and the second is called Bob.
When the send request, Bob name is typed by Alice and her public key is fetched from the local storage then the request is sent to the server.
When a request is received, it appears as a notification (Fig. 4). If the friendship request is accepted by Bob, his private key is fetched with Alice's public key to calculate the session key by using Elliptic Curve Diffie-Hellman (ECDH) over the curve Curve25519 [18] and hashes the result with HSalsa20 [15] then the session key is stored in

local storage (Fig. 5). In the end, the acceptance is sent with his public key to the server to be delivered to Alice.
Upon receipt of the acceptance of the request, the same steps on the above are taken. The session key is calculated by using Alice private key and Bob public key then it is stored in the local storage for later use.
The session key is the same for both parties and this is the strength of the Elliptic Curve Diffie-Hellman (ECDH) and thus it is difficult to attack by the man-in-the-middle. In addition to, the weakness of the traditional Diffie-Hellman has been eliminated.

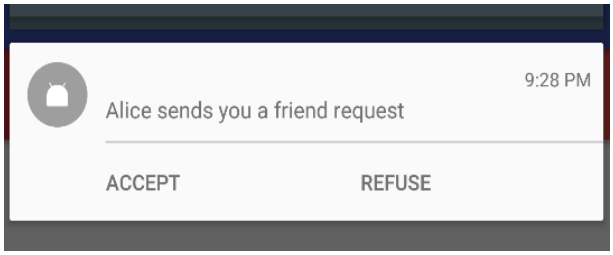

Fig. 4. Friend request notification.

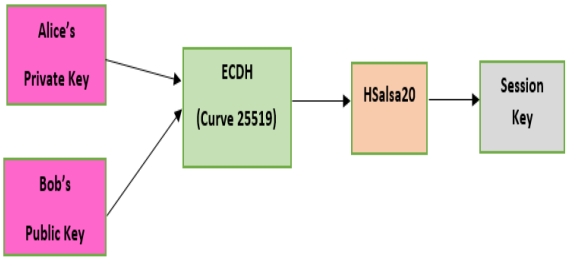

Fig. 5. Session key Setup.

3.7 Exchanging Messages

When a message is typed, the application encrypts the message using XSalsa20 encryption algorithm to encrypt the message body and Poly1305 to compute a Message Authentication Code (MAC) [19]. Each message has its own separate key and nonce which brings better security for each single message in such discovering one of the keys cannot decrypt previous messages. After encrypting the message, it is encrypted again using the recipient's session key then it is sent to the server (Fig. 6).
After the message is received from FCM, the MAC of the encrypted message is calculated and compares it with the received MAC to verify the integrity of the message. If the results are not the same, it is rejected and does not show to the user otherwise it is decrypted by the sender session key. Next, the message body is verified in the same steps above. Now the key and nonce to decrypt the message are known. The message is then decrypted and stored in the local storage and displayed to the recipient.

If the application is in the background the message will be displayed as a notification while if the recipient uses the application it will be displayed in the chat window.

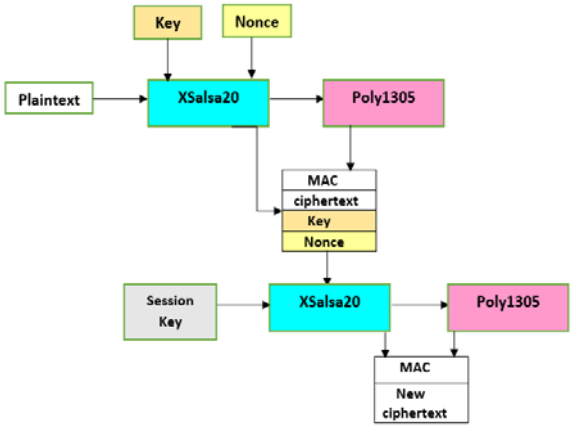

Fig. 6. Procedure to encrypt a message.

3.8 Local Storage

The data is stored locally in the application by using Realm database. Realm is a lightweight mobile database that supports cross-platform. It's easy to use and fast. More, it has lots of modern features such as JavaScript Object Notation (JSON) support, a fluent API, data change notifications and encryption support [20]. Encrypted data is protected from unauthorized access and is accessible only if have been a right encryption key. Realm uses AES-256+SHA2 algorithm and 64-byte key for encrypting storage [21]. To prepare Realm storage passes through several steps that are:
Step 1: The application checks whether the lock screen is present or not. If it exists, the following steps are completed.
Step 2: Generate Realm Key that is used for encrypting storage.
Step 3: Generate key from Keystore.
Step 4: Realm key is encrypted with the key generated in step 3 by using AES in CBC mode.
Step 5: Save the encrypted key in shared preferences in private mode so that other applications cannot access this data directory.
Three files are stored in the local storage. UserInfo file that stores all information pertaining to the user. While Friends file stores all information pertaining to the friends. Finally, Messages file stores all information pertaining to messages.

3.9 Server Side Implementation

Server-side has relied on Node JS[22] and MongoDB database[23]. Node JS is fast, capable of handling a large number of simultaneous connections with high throughput, which is equivalent to high scalability. MongoDB and Node JS have often used together because of their using

JSON so no need to spend time for transforming the data between them making it easy to deal with each other. In addition, MongoDB provides TLS that makes a secure connection (Fig. 7).

To perform a client request passes through several steps that are:

Step 1: Initially, must run the MongoDB connection then run the Node JS from Command Prompt. At this stage, the server is ready to receive the client's request.

Step 2: When the client sends a request, the server receives the HTTP request in JSON format. The request then parsed.

Step 3: The HTTP request is compared with the base path if it is matched, it is handed to Express framework.

Step 4: The Express receives the HTTP request and routes it to the specific endpoint that matched it. In case of not matched with any of the routes will display error in Command Prompt. Otherwise, it will be forwarded to the controller which handles the required function.

Step 5: Make a request to MongoDB database by mongoose for processing function.

Step 6: When the data is fetched from MongoDB database and the required operations are done, Node JS receives the response then sends to the client.

The above steps are shown in Fig. 8.

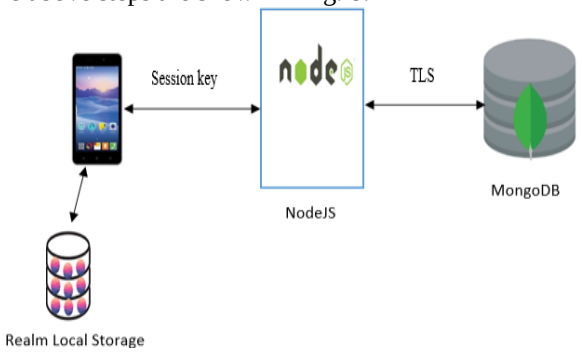

Fig. 7. The Specific Architecture of Proposed Chat.

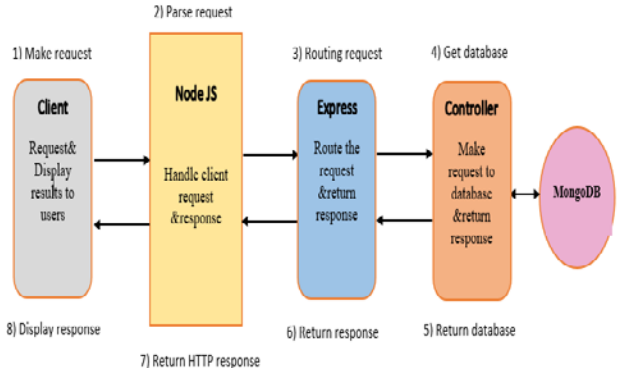

Fig. 8. Implementation of a client request.

4. Analysis the Proposed Chat

In section 3, we listed a set of requirements for securing chat. To analyze and evaluate proposed chat we have compared proposed chat with popular applications discussed in section 2. The comparison is based on the requirements listed in Table 1.

Table 1. Comparison with Popular Chat Applications

Criteria	Whats App	Viber	Telegram	Facebook Messenger	Propose d Chat
Req1	N	N	N	N	Y
Req2	Y	Y	Y	Y	Y
Req3	Y	Y	P	P	Y
Req4	Y	N	N	P	Y
Req5	Y	Y	N	N	Y
Req6	N	N	N	N	Y

Note:"Y" it means that it meets the requirement. "N"does not support the requirement. "P"only the secret part supports it.

5. Conclusion

In this paper, we introduced a specification for preserving the security and privacy of the chat application. We described a set of requirements for making secure chat and implement it by using modern methods and lightweight for providing speed and good protection to its clients. XSalsa20 algorithm ideal for mobile devices because of its high security, high performance and maintains battery life. Clients can be confident that nobody can read their messages, even if the mobile phone reaches wrong hands cannot enter to the application and cannot access the data stored locally.

References

[1] Ash Read, "How Messaging Apps Are Changing Social Media," 2016. [Online]. Available: https://blog.bufferapp.com/messaging-apps.

[2] Most popular messaging apps 2017 | Statista," 2017. [Online]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

[3] D. Moltchanov, "Client/server and peer-to-peer models: basic concepts," 2013.

[4] Martin Kleppmann, "The Investigatory Powers Bill would increase cybercrime — Martin Kleppmann's blog," 2015. [Online]. Available: https://martin.kleppmann.com/2015/11/10/investigatory-powers-bill.html.

[5] D. P. Roel Hartman, Christian Rokitta, Oracle Application Express for Mobile Web Applications - Roel Hartman, Christian Rokitta, David Peake - Google Books. 2013.

[6] Viber Encryption Overview." [Online]. Available: https://www.viber.com/security-overview/.

[7] WhatsApp inc, "WhatsApp security whitepaper," p. 10, 2017.

[8] "Telegram F.A.Q." [Online]. Available: https://telegram.org/faq.

[9] T. Susanka, “Security Analysis of the Telegram IM,” p. 70, 2016.
[10] B. O. B. Kamwendo, “Vulnerabilities of signaling system number 7 (ss7) to cyber attacks and how to mitigate against these vulnerabilities. bob kamwendo,” vol. 7, no. 7, 2015.
[11] John Leyden, “SS7 spookery on the cheap allows hackers to impersonate mobile chat subscribers • The Register,” 2016. [Online]. Available: https://www.theregister.co.uk/2016/05/10/ss7_mobile_chat_hack/.
[12] “Active Sessions and Two-Step Verification.” [Online]. Available: https://telegram.org/blog/sessions-and-2-step-verification.
[13] T. Whitepaper, “Messenger Secret Conversations,” 2016.
[14] “Android Keystore System | Android Developers.” [Online]. Available: https://developer.android.com/training/articles/keystore.html.
[15] D. J. Bernstein, “Extending the Salsa20 nonce,” no. Mc 152, pp. 1–14, 2011.
[16] M. B. Jones, “The Emerging JSON-Based Identity Protocol Suite,” 2011.
[17] “Firebase Cloud Messaging | Firebase.” [Online]. Available: https://firebase.google.com/docs/cloud-messaging/.
[18] D. J. Bernstein, “Curve25519 : new Diffie-Hellman speed records,” vol. 25519, 2006.
[19] D. J. Bernstein., “Poly1305.” [Online]. Available: https://en.wikipedia.org/wiki/Poly1305.
[20] “Realm: Create reactive mobile apps in a fraction of the time.” [Online]. Available: https://realm.io/.
[21] “Realm Swift 2.10.2.” [Online]. Available: https://realm.io/docs/swift/latest/.
[22] “Node.js.” [Online]. Available: https://nodejs.org/en/.
[23] “NoSQL Databases Explained | MongoDB.” [Online]. Available: https://www.mongodb.com/nosql-explained.