Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.

End-to-End Security and Privacy PreservingMobile Chat Application

Pulkit Jain[1], Vishal Saini[2], Yash Kumar[3]

[1]Galgotias University. 12pulkit.jain@gmail.com
[2]Galgotias University. vishalsaini3498@gmail.com
[3]Galgotias University. yashk5843@gmail.com

Abstract - Since 1990s, technology have reshaped how we saw and enjoy the arena around us. These technologies are Internet and cellular communications, particularly smartphone. The Internet provides at a reasonable price and handy manner to discover and talk with people who are far from us. A throng of offering had converged at the cell phone platform, and without a doubt the maximum high-quality is social networking. Giving fast internet connectivity and use of online offerings, issues like protection and privateness are growing. In this paper, we examine the issues of protection and privateness retaining functions furnished with the aid of using present mobile chatting application. This paper additionally puts forward a simple framework for an End-to-End protection and privateness retaining mobile chatting service requirements related to it. We carried out the concept to provide proof of idea and examine the technical difficulties coming in order to achieve protection and privateness.

INTRODUCTION

The immediate messaging services provided by different applications like WhatsApp, Messenger are overtaking conventional messaging services, turning into the desired medium of conversation for tens of thousands of mobile users. However, the security and privacy keeping functions of different cellular programs had come below the spot-light. There are different protection and privateness functions furnished via way of means of different cellular chat programs, however there aren't many chatting application that offer an End-to-End security and privacy keeping carrier to their customers.

In this paper mainly, we focus on this sort of cellular chatting carrier. We suggest a framework for constructing this sort of carrier after which compare the technical demanding situations worried in enforcing it, to offer a proof of idea and apprehend any possible technical troubles which can also additionally limit such functions from being carried out via mainstream cellular chat carrier providers.

CONTRIBUTION OF PAPER

Paper mainly offers with the safety and privacy associated demanding situation confronted in the designing, improvement and securing of cellular chatting services. The fundamental contributions of this are:

1. Secure key exchange for offline messages.
2. End-to-End safety and privacy maintaining structure for cellular chat services provider.
3. Implementation evaluation of proposed structure.
4. User-to-User authentication and authorization mechanism.

CELL PHONES

In this part, at length we visit to cell phone era as a way to recognize the dimensions of the market, which at once pertains to the safety and privateness issues of cellular chat users.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.

SMARTPHONES: A PARADIGM SHIFT

The smartphone platform has advanced a protracted manner from the authentic easy medium of voice and textual content verbal exchange to come to be the main hub of the virtual world. Cell phones, together being a leisure hub, had additionally evolve right into a social construct that had affiliation and emotional attachment for individual. It is likewise turning into the fundamental medium for making connection with the sector through social media application. Users uses a cell chat carrier to talk with every other, a process that could consist of diffuse non-public information. The protection and privateness of such communication have to be taken very seriously. However, current episode of vulnerability with inside the needed chatting services monitor that they may not be strictly imposing protection and privacy features. In the subsequent section we briefly find out the variety of chatting applications to be available on Android and iOS. This discussion offers an evaluation of existing services withinside the business area. We speak present educational paintings associated with protection and security retaining chat software program. The choice of commercially available chat software program was made in a way that reflect the prevailing approach, and it is by no means an entire list.

WHATSAPP

WhatsApp app is taken into consideration to be one of the largest cellular chat applications available on different platform. The structure of the provider is proprietary and the information on this phase are taken from quite a number of valid resources. The fundamental or basic awareness of the product is on sending or receiving messages and privacy worries are secondary. WhatsApp does not keep any message at the server station, the chats record is saved in the customer device only. The customer utility makes use of SSL to hook up with the server. However, a latest weblog posting mentioned about the deployment of SSL model. The deployment of this model would possibly open WhatsApp to assaults on SSL. There is not any E2E encryption which offer safety in chatting among senders and receivers. Therefore, the message server can examine the messages exchanged.

WICKR

The maximum latest addition to the variety of secure chat application is Wicker. Although most of their structure is proprietary, in this phase we talk the functions they declare to offer to user. They declare that they always encrypt every individual message, using a cryptographic generated key. However, it is very difficult to decide whether or not those keys are generated by the message server or the users. They most effectively declare that customers personal key isn’t communicated to the server. Furthermore, it is claimed that tool, region and meta fact approximately customer and message are covered, supplying a very strong privacy mechanism. Communication among the tool and the chatting server is covered via way of means of TLS.

RELATED WORK

Security and privacy troubles when it comes to clever telephone have acquired considerable attention in regards to cellular chat packages. Although there are a number of cellular chatting applications that declare to offer a steady and secure service, their whole structure isn't publicly available. To our fine knowledge there aren't many guides that describes such structures. Securing textual content messages structures had a robust foundation in proposals like Media Path Key Agreement for Unicast Secure RTP, Off-the-Record and A Secure Text Messaging Protocol. In this very paper, we aim to provide a potential

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.
structure which takes care of both protection and privacy to offer a whole structure, there by filling the gap with inside the current work in the area of cellular chatting application.

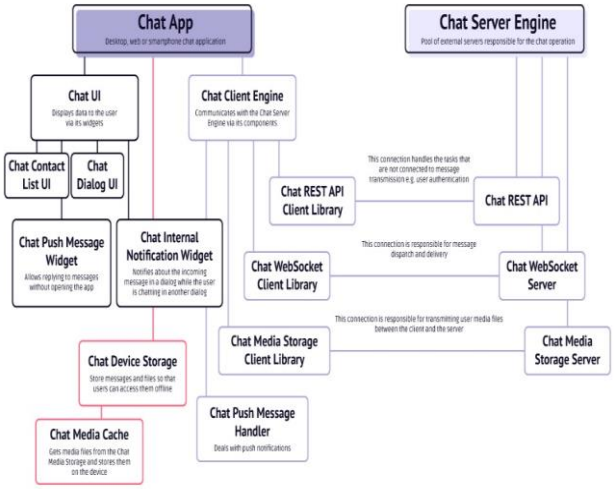
Secure And Privacy Preserving Mobile Chat

In this part, we firstly discuss the security and privacy requirements of mobilechat application. In the remaining part of the discussion, we saw a in detail proposed architecture and describes its features.

Secure And Privacy Preserving Mobile Chat Requirements

Before we present the details of the proposed architecture for mobile chat applications, this section provides a brief list of requirements that any such proposalshould meet:

Req1 The signing up process must require minimum information related to the user. The account set up or creation process should not rely fully on Personal Identity Information
Req2 The secret key exchange process must be safe, intact and support chat without any internet connection.
Req3 Encrypting/decrypting of message should require least interaction of user.
Req4 Secure offline message can be communicated safely along with potential key share



Req5 Individual user had a mechanism to authenticate each other, which assures themselves that they are communicating with the right person.
Req6 Communications should not store on the chat server. Individual chat sessions can be stored on the user's device
Req7 Local chat storage should be adequately protected
Req8 To safeguard the privacy of the users and their messages, the chat server must not be able to retrieve the chats.

PROPOSED ARCHITECTURE

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.
The conventional structure of a steady and privacy-retaining cell chat application is proven. After successfully installing a cell chatting utility, the person of cell 'X' initiates the signing up manner. The signing up manner will be used both to make a brand-new user account or to register the usage of a present account using credentials. The chatting server, which includes a club server and a message server, initiate the account's introduction manner. The club server manages the person's account, related credential and the person's contacts list. The chat server handles the messages verbal exchange among users, whether or not each user is online, if the supposed receiver is offline. If the receiver is offline, the messages might be saved withinside the offline chat store. These chats are briefly saved and as soon as they're added to the respective receiver they are deleted. The broken line represents digital verbal exchange among the customers of mobile 'X' and 'Y', thru the chat server. The verbal exchanges hyperlink among the cell utility and the chat server is covered the usage of cryptographic keys. In addition to, the digital verbal exchange hyperlinks among the customers of mobile 'X' and 'Y' are encrypted the usage of the cryptographic generated keys and acknowledged every effective to the respective application (of customer 'X' and 'Y').

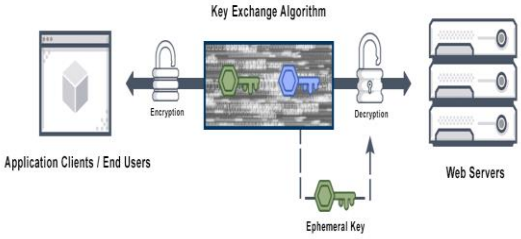
Signing Up

In the cell application request and authentication by the chat service provider, it issues cryptographic keys or certificate to both of the private key and the public key of the application In succeeding communication between the cell chat application and the chat service provider, a unique alphanumeric user-id and cryptographic key certificate is used to authenticate and authorize the user and application and establish a TLS session which is a two-way authentication and authorization based on SSL or TLS sessions.

Key Exchange

There are four random numbers included inside the secret message which are used to generate individual message keys that we discussed earlier in the cryptography part. At the final step, the last block contains the master key or symmetric key that the sender of the message required the receiver of the message will be using it during any future communication. Clock synchronisation between the communicating users is not required to use the time stamp, because when a cell phone application connects to the chat service provider, it gets a time which is also known as server time and use it as an internal but small application. The only major difference in a group chat is that the chat organiser which also known as group administrator will generate the main master key and share it with all participant of that group, participants will then use this master key to encrypt all their chats. In this situation, if a single user of that group is offline then either he or she might not be able to read chats exchanged in the group messages else he or she has to be removed from the group if the chatting session has to be continued for long enough.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.



Chat Communication

Each and every message send by a particular user is encrypted by different keys, which are generated using the shareable master or public key and any four numbers which are random. In this part, we will briefly discuss how individuals' message are generated and how the shared public key is used to generate message key. For the messages which are coming to user and for the exiting messages, each communication entity would have at least two different shareable master or public key and seeding files. The shareable numbers which are four random numbers are taken as the seed files, for every cycle of function a random number will be encrypted using the shared master keys.

Implementing In the Real World

Using the above proposed features of the mobile chatting application in the earlier section, we saw the detailed basic implementation which is carried out to provide a proof for the concept, for the proposed features. In this part, we mainly discuss the real-life implementation.

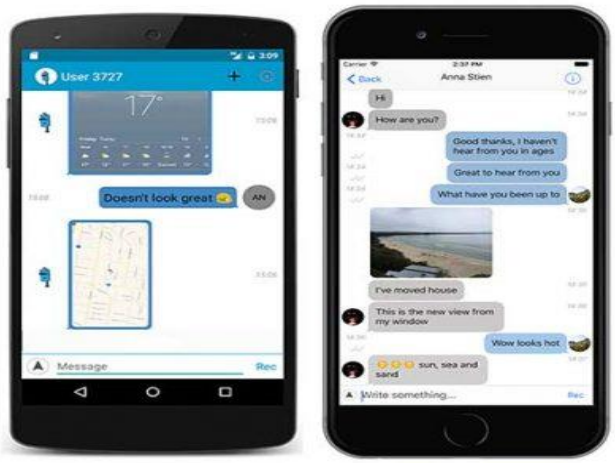
Technology Overview

The earlier chatting server was hosted on the processor Intel 9 Core i7, 2.70GHz with 8GB Random Access Memory the machine will run Ubuntu 10 13. In all subsequent section, we briefly discuss the practical experiences for both the chat service provider and the cell phone applications. The installing of a highly secure chatting service requires the practical execution of the chatting server and the cell phone application.

Server-side Execution

We have chosen Mosquito tool for its practical execution of MQ Telemetry Transport and the rationale behind the choice of MQ Telemetry Transport is MQ Telemetry Transport provided several useful features, such as push notifications so that continuously polling for new chats is not required by the Android based chatting app, confident or authorized messages delivery and reliable, low battery consumption, and also "offline message delivery". With the of MQ Telemetry Transport means that chat message is smaller in size than the same message created with other messages protocol such as Extensible Messaging and Presence Protocol, using MQ Telemetry Transport generate 70 bytes, whereas the same message in Extensible Messaging and Presence Protocol is represented with 100 bytes. MQ Telemetry Transport also provide smaller chat sizes due to being a binary protocol, comparing to other protocol like Extensible Messaging and Presence Protocol, which uses Extensible Markup Language for its texts.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 7, 2021, Pages. 42- 50
Received 05 May 2021; Accepted 01 June 2021.



Screen Shot of Mobile Chat Application Running on Two Android Devices

Mobile Side Execution

For cell phone chat, we developed an app which supports Android 4+. Additional Programming Interfaces included GSON for changing JSON, SQL Cipher for fully encrypted databases, Eclipse Pan American Health Organization for MQ Telemetry Transport messaging and Spongy Castle for cryptographic algorithm.

OVERALL ANALYSIS

In this section, we will be discussing briefly the construction and execution of our secured mobile chatting service.

Analysis Of the Suggested Architecture

we listed the basic requirement for a secured and privacy preserving chatting service provider. It is clear that our proposals meet all the requirement, and that is one of the most extensively used mobile chatting service, "WhatsApp" does not fulfil even one and half of the requirement. Taking these some of the main requirement, we had equipped a comparison between our suggested and socially available product discussed in above sections.

Implementation Analysis

The main motive of the execution was to provide a proof for the concept used for the main architecture of a secured and privacy providing mobile chatting applications with publicly available specifications. We only the applications for its feature and whether or not it adequately supports all the requirements listed above. In addition to this, we didn't test the scalability of the execution of the chatting service provider. However, with regards to text generating message, the implementations were comparable to any socially available mobile chatting applications. However, we could not profess the same for the chatting server as we did not simulate the loading test to make it comparable to other cell phone chatting service. Therefore, the exercise was to mainly study the technical difficulties that a chatting service providers might face while developing such services.

CONCLUSION

In the whole paper, we mainly provide open specifications for a more secured and privacy securing chatting services. We briefly describe the basic requirement, architectures and execution experiences in installing such services. The main aim of this paper isto develop a mobile chatting service and explores as many as potential complex methodology involves in this kind of services which provides privacy protection to its users. In this paper, we traversed the theoretical foundation and all the technical challenge faced by the team if privacy defence is built into a chatting service. We found that most of the theoretical and technical component are already available. With a few minor modification, a strongly privacy-preserving based chat service can be built. We have shown thata secure and privacy-preserving chatting application is technically feasible. Duringthe implementation of the framework, we didn't face any major issues related to the technologies or performances that might make this suggestion infeasible. Whether it is viable business or not but is a different aspect for such services, and was not considered in this study. In the coming research, we would like to do experiments with the scalabilities and performances of the chatting service provider or server, this might reveal some bottlenecks in building andmaintaining a privacy-centred chatting servers. Another potential aspect is investigating of how the texts in chatting services proposed in this study could be extended to a video or audio chatting service. The challenge presented in providing a secured andprivacy-preserving audio and/or video chatting services might be more than those presented by a text-based chatting services. This will give a much better insight into the development of secured and privacy keeping service, their running cost and usability requirement, providing an opportunity to understand the underlyingreasons why such service are not prevalent or widely adopted by users.

REFERENCES

1. Thomas, D., Bradshaw, T.: Rapid Rise of Chat Apps Slims Texting Cash Cow for Mobile Groups. Online. Financial Times (April 2013), http://www.ft.com/intl/ cms/s/0/226ef82e-aed3-11e2-bdfd-00144feabdc0.html#axzz2urfG5LDi

2. Paczkowski, J.: WhatsApp: Bigger Than Twitter. Online. All Things D (April 2013), http://allthingsd.com/20130416/whatsapp-bigger-than-twitter/

3. reenwald, G.: English NSA Collecting Phone Record of Millions of Verizon Cus- tomers Daily. Online. The Guardian (June 2013), http://www.theguardian.com/ world/2013/jun/06/nsa-phone-records-verizon-court-order

4. Vincent, J.: Affiliations, Emotion and the Mobile Phone. In: Esposito, A., Vích,

   R. (eds.) Cross-Modal Analysis. LNCS (LNAI), vol. 5641, pp. 28–41. Springer, Heidelberg (2009)

5. Ling, R.: New Tech, New Ties: How Mobile Communication Is Reshaping Social

Cohesion. The MIT Press (2008)

6. Laugesen, J., Yuan, Y.: What Factors Contributed to the Success of Apple's iPhone? In: Proceedings of the 2010 Ninth International Conference on Mobile Business / 2010 Ninth Global Mobility Roundtable ICMB-GMR 2010, pp. 91–99. IEEE Computer Society, Washington, DC (2010)

7. Akram, R.N., Markantonakis, K., Mayes, K.: Building the Bridges – A Proposal for

   Merging different Paradigms in Mobile NFC Ecosystem. In: Xie, S. (ed.) The 8th International Conference on Computational Intelligence and Security (CIS 2012). IEEE Computer Society, Guangzhou (2012)

8. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., Glezer, C.: Google

   Android: A Comprehensive Security Assessment. IEEE Security and Privacy 8(2),35–44 (2010)

9. Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile

   Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: 2011 IEEE Symposium on Security and Privacy (SP), pp. 96–111. IEEE (2011)

10. Goodin, D.: Crypto Weaknesses in WhatsApp "The Kind of Stuff the NSA would

    Love". Online. ARS Technica (February 2014), http://arstechnica.com/ security/2014/02/crypto-weaknesses-in-whatsapp-the-kind-of-stuff-the-nsa-would-love/

11. The WhatsApp Architecture Facebook Bought for $19 Billion. Online. High Scal- ability, (February 2014) http://highscalability.com/blog/2014/

    2/26/the-whatsapp-architecture-facebook-bought-for-19-billion.html

12. Freier, A., Karlton, P., Kocher, P.: RFC:6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0. Online. IETF (August 2011)

13. Security of BlackBerry PIN-to-PIN Messaging. Online. Communications Security

    Establishment Canada, http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb57b-eng.html (March 2011)

14. Dierks, T., Rescorla, E.: RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2., Tech. Rep. (August 2008)

15. Moscaritolo, V., Belvin, G., Zimmermann, P.: Silent Circle Instant Messaging Pro-

tocol: Protocol Specification, Online, White Paper (December 2012)

16. Landman, M.: Managing Smart Phone Security Risks. In: 2010 Information Secu- rity Curriculum Development Conference, pp. 145–155. ACM (2010)

17. Felt, A.P., Egelman, S., Wagner, D.: I've Got 99 Problems, but Vibration ain't

One: A Survey of Smartphone Users' Concerns. In: Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 33–44. ACM (2012)

18. La Polla, M., Martinelli, F., Sgandurra, D.: A Survey on Security for Mobile De-

vices. IEEE Communications Surveys & Tutorials, 446–471 (2013)

19. Zimmermann, P., Johnston, A., Callas, J.: ZRTP: Media Path Key Agreement for Unicast Secure RTP. IETF, RFC 6189 (April 2011)

20. Alexander, C., Goldberg, I.: Improved User Authentication in Off-the-record Mes- saging. In: Proceedings of the 2007 ACM Workshop on Privacy in Electronic Soci- ety, WPES 2007, pp. 41–47. ACM, New York (2007)

21. Belvin, G.: A Secure Text Messaging Protocol. Cryptology ePrint Archive, Report 2014/036 (2014), http://eprint.iacr.org/

22. Dyreson, C.E., Snodgrass, R.T.: Timestamp semantics and representation. Infor- mation Systems 18(3), 143–166 (1993)

23. Akram, R.N., Markantonakis, K., Mayes, K.: Pseudorandom Number Generation in Smart Cards: An Implementation, Performance and Randomness Analysis. In: Mana, A., Klonowski, M. (eds.) 5th International Conference on New Technologies, Mobility and Security (NTMS). IEEE Computer Society, Turkey (2012)

24. Rogers, R., Lombardo, J., Mednieks, Z., Meike, B.: Android Application Develop- ment: Programming with the Google SDK. O'Reilly, Beijing (2009) Apache, Apache Tomcat (May 2007) http://tomcat.apache.org/