A Review on Cryptographic Techniques and Security Protocols over Instant Messaging Applications

Nosheen Nazir, Muhammad Sheraz Arshad Malik, Ijaz Shoukat, Javeria Mehboob, Aliya Yousaf and Samina Naseem

Department of Computing, Riphah International University, Faisalabad, Pakistan

Abstract
For secure mobile communications users rely on Instant Messaging applications (IM), massive volume of private and personal data is shared over the network, the questions on discretion and sanctuary of private data are raised for secure transmissions. Exclusive antidote to this snag is deployment of cryptographic techniques and proficient security protocols in IM applications. This research reviews applied end-to-end encryption techniques and protocols in distinguished applications i-e. WhatsApp, Viber and Telegram. This study also investigates employed Signal, MTPro protocols starting from Off-The-Record (OTR) and most secure IM application is suggested after comprehensive analysis.

Key words
Secure Communication, Cryptographic Techniques, Secure Messaging in Mobile Devices, IM Techniques & Protocols

1. Introduction

Instant Messaging (IM) is an online service for communication between two or several clients including text messaging, Voice Over Internet Protocol (VoIP), broadcast messaging or multi-media sharing that takes place over an internet[1, 2]. It is one of the most frequently used service that is a giant source of information sharing for communication among mobile devices [3]. IM is not only a basis of communication but have become status symbol of modern society reflecting their ways of standardized living [4].

With the advent of technology i.e. Smartphones, iPad, iPhone etc. simple text messaging (SMS) has been replaced by social networking applications such as WhatsApp, Viber, and Telegram etc. [5]. The number of users are increasing day by day and enormous amount of personal and secret data is being shared, even WhatsApp alone is responsible for carrying out 50 billion of messages (text, audio, video, contacts, locations etc.) per day [6]. The main reason behind the use of such applications is that they are freely available to download and can be installed without any restriction and just require simple information for registration [6].

With speedy change in mobile technology and due to lack of security measures and privacy flaws in social IM applications, the shared data is exposed to risks of being hacked, snoofing and vulnerable to threats of mis-use of confidential data. It intensely urged the need of developing secure IM applications particularly for the purpose of reliable communications [7, 8].

The solitary solution to the existing security and privacy concerns for online transmissions is cryptography. "Cryptography is an art of scrambling simple text (plaintext) via encryption into complex and unidentifiable text (cipher)" with aiming at chief objectives of confidentiality, authentication, non-repudiation and integrity. It lays the foundation for secure messaging and almost all IM apps declare that they provide end-to-end encryption features and thus securing the personal, valuable and treasured data of clients from cybercriminals [4].

Secure communication between two persons/parties via instant messaging applications instantiated the crucial need for end-to-end encryption, and it is recently adopted by almost all popular IM apps thus securing the privacy of their valuable customers. In end-to-end encryption, the simple text that need to be shared by sender is known as plaintext and encrypted text after application of encryption algorithm is known as cipher. The receiver decrypts cipher into plaintext (decryption) via use of same or different algorithm [9, 10]. The main component through which encryption decryption is possible is referred to as "Key". On the basis of Key, Encryption is subdivided into two types i.e. Symmetric Encryption (Private Key Cryptography) and Asymmetric Encryption (Public Key Cryptography).

In Private Key Cryptography, the same key is used by sender and receiver for encryption and decryption. Drawback of this scheme is "secure key-management". They are further categorized into block algorithms and stream algorithms. Common examples include DES, AES, RC2, RC4, RC5, RC6, IDEA, MARS, Triple-DES etc.[11].

In Public Key Cryptography, if sender encrypts using his private key, the receiver decrypts the cipher using his public key, thus different keys are used for encryption and decryption. Thus this scheme is more reliable and common Asymmetric encryption algorithms include

Manuscript received August 5, 2018
Manuscript revised August 20, 2018

Deffie Hellman, RSA, ECC and Digital Signatures as well [9, 11, 12].

IM apps are assumed to satisfy privacy and security concerns by incorporation of confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, anonymity perseverance, global transcript, message unlinkability, repudiation, backward secrecy, resilience etc. [13].

The main contribution of this paper is to provide a clear review of popular Instant Messaging Applications i.e. WhatsApp, Viber and Telegram based on their utilized encryption techniques and network security protocols. Rest of the paper is organized as: Section 2 discusses the related work with respect to several IM applications and protocols used by them earlier for secure communications and Section 3 presents detail on Instant Messaging, Section 4 elaborates IM Encryption techniques and protocols in popular applications, and Section 5 summarizes the whole research in the form of results.

2. related work

A wider research has been carried out for the purpose of security and privacy in IM applications through encryption and is discussed as below:

All messaging services are accessed in client-server mode, so the user relies on network operators for the security of their communication and the best solution for secrecy of messages is to do encryption, particularly end-to-end encryption, with forward secrecy in which sender sends the encrypted message and is only decrypted by intended receiver. Popular IM apps i-e WhatsApp, Telegram and Viber have incorporated end-to-end encryption facility with Signal Message Protocol (SMP) with two modes i.e. opportunistic end to end encryption mode and authentication end to end encrypted mode. The first mode provides user authentication via key exchange with involvement of operator. In the subsequent mode, user performs authentication ceremony by himself [14, 15]

Off-The-Record (OTR) was one of the first IM protocol used for user authentication and by involving shared public keys or paraphrase, integrity and confidentiality were achieved and end-to-end encryption was possible. This technique made utilization of asymmetric encryption but was unable for decryption of past messages [16] Signal is another end to end encryption protocol providing "future secrecy" empoused by WhatsApp, Messenger grounded on PKI (Asymmetric Encryption) and employs DH key exchange as the core algorithm[16].

In [9], "keyword mono alphabetic substitution algorithm" based on AES (Advanced Encryption Standard) is used for encryption and decryption. This proposed technique for secured messaging is equally suitable for real time apps, chats, messages etc. irrespective of platform dependency with reduction in processing overhead to maintain security, but it is lesser secure than PKI (Public Key Infrastructure).

In [17], for security and privacy concerns several techniques of data privacy were analysed and compared with each other including K-anonymity (AES, IDEA etc.), Homomorphic encryption (HE) subdivided into Partial Homomorphic Encryption and Full Homomorphic Encryption leading to production of aggregation services, Group Signatures (GS) allowing user to authenticate himself on behalf of group, Attribute Based Signature (ABS) based on attribute tree, Attribute Based Encryption (ABS) based on key-policy ABE and ciphertext-policy ABE, Ring Signatures (RS) securing sender privacy by elimination of certification requirement. But limitation of these techniques is that they sometime can lead to large digital signatures so the encryption/ decryption process becomes expensive in terms of memory usage.

When a single user have multiple devices than, sharing/distribution of private keys is vulnerable to threats, for this reason, Shatter-an open source platform is presented that utilizes threshold cryptography. Vital component of Shatter is library based on two algorithms i.e. Threshold DSA with OTR protocol and Damgaard-Jurik threshold with Paillier's HE algorithm. It made easier the distribution of DS and end to end encryption process, also achieved backward compatibility and implemented the proposed platform on eminent apps i.e. OmniNote and ChatSecure. But its application is limited to the defined threat model and is platform dependent [18].

In [19], authors presented PAgIoT protocol that performs tasks related to privacy perseverance aggregation under Pallier Cryptosystem and outperforms existing protocols i.e. HDA, iCPDA. This protocol is resistant to eavesdropping and collision attacks.

In [20], authors presented non-interactive DAKE (Deniable authenticated Key Exchange) protocol which is an extension of AKE (Authenticated Key Exchange), this protocol put forth "forward secrecy" with deniability properties in offline and online modes, thus resulting in secure messaging over synchronous communications. On the other hand OpenPGP and S/MIME[13] are well known protocols that does not ensures message repudiation and usability issues are encountered yet participant repudiation is performed. Moreover, authors have discussed Dual Receiver Encryption (DRE), Non-Committing Encryption (NCE), RSDAKE (Ring Signature DAKE) and SPAWN as well, and all the four discussed protocols performed differently in terms of usability and security.

In [13], the authors addressed three main concerns i.e. trust establishment, conversation security, and transport privacy. They evaluated trust establishment by opportunistic encryption, TOFU, key finger print verification, SAS, SMP, QR Codes, blockchains,

Certificate Transparency Protocol, transparency logs. Conve3rsation security is achieved mainly by integrity, confidentiality, authentication with respect to AKE, DH, FS-IBE, 3-DH Handshake. Transport privacy is evaluated on grounds of store-and forward, Onion Routing, DC-nets, PIR protocol.

On the other hand, Secure Electronic Transactions (SET) protocol offers authentication, integrity, linkage as well as confidentiality by utilization of PKI and certificates. S/MIME provides Encryption through DH, RSA, 3-DES, and Digital Signatures through SHA-1 and MD-5[21, 22].

In [4] For secure IM, Four applications of cryptography i-e. KryptoKaz, EnDe Crypto, AES Crypto, Encrypt, running on distinct platforms were tested with defined parameters of randomness, avalanche effect, key space, and kerckhoff principle. All the applications developers claimed that their applications are based on AES algorithm as it is regarded as best security standard by NIST. But Encrypt proved to be best in all tests subsequently followed by AES Crypto and EnDe Crypt.

3. instant messaging

According to Cambridge Dictionary, Instant Messaging is defined as "A type of service available on the internet that allows you to exchange written messages with someone else who is using the service at the same time" Instant Messaging enables a person to communicate through online chats where one can share text messages, audio, video, live streaming, files, web links etc. between two or more persons. Instant Messaging apps are connected to social networking websites where same software is shared amongst clients. Internet is the backbone behind such applications and these can be run across several platforms including personal computers, smart phones, iPhone etc.[4, 23-25]

4. in encryption techniques and protocols

In cryptography, encryption is defined as such a process in which information sharing is muddled to make it unreadable for transmissions over insecure channel (usually network) such that man-in-middle attack, eavesdropping, spoofing etc.

could be prevented. [10, 26-28]. There is no chance of surveillance, tapping, peeping because of un-sharable characteristic of cryptographic keys for the data being stored [24]

4.1 WhatsApp

Popular Instant Messaging applications that have acquired much of users interest include WhatsApp, Viber, Telegram [24].WhatsApp is the most highly rated application with largest number of users. It ensures E2EE via Signal protocol, deniability through OTR, and DH is used as Key-Exchange method. For the purpose of achieving "forward secrecy" ECC-25519 with ECDH Key Agreement is implemented. Since highly resistant to MITM attacks [29, 30]. HKDF is a function for key derivation in which "Root Key and Chain Key" are derived from master_secret [30].

4.2 Viber

Salsa20 Stream Cipher is the core algorithm used by Viber along with ECDH and SHA-256 based on Double Ratchet for gaining forward/backward secrecy and authentication [31]. For encryption of Viber calls 256-Bit Curve25519 is implemented [32].

4.3 Telegram

MTPro protocol is used by Telegram (IM app), is based on block cipher, therefore comprises of padding. In case of active attacks, symmetric encryption must confront to the AE and IND-CCA definitions, but this study revealed that MTPro do not satisfy these definitions, and thus is susceptible to security threats. It is comparatively less efficient Authentication Encryption rather AES parallel with HMAC

can stipulate enhanced authentication. Later on a modified version of MTPro was suggested in [33] that utilized AES-CTR instead of AES-IGE with an improvement in parallel processing and it was more secure as compared to the earlier one[33, 34].

Table 1: Comparison of WhatsApp, Viber, Telegram

	WhatsApp	Viber	Telegram
End-to-End Encryption	✓	✓	✓
E2EE Notification	✓	×	✓
Key Change Notification	✓	×	×
Re-encrypt/Send In-Transit Notification	✓	×	×
QR-Code	✓	✓ (only for secondary device)	×
2-Step Verification	✓	×	✓
Verification through call	✓	×	×
Security Protocol	Signal	Similar to Double Ratchet used in Open System Signal Application	MTPro

Security Of Screen	✕	✕	✓
Encryption Technique	Double Ratchet	Double Ratchet via 128 Bit symmetric Key	Symmetric AES with block chain in IGE
Transmitting Media	AES 256 Key, HMAC-SHA 256, ECDH	Salsa20 Encryption algorithm, Double Ratchet algorithm,	--
Protocol for Calls	SRTP	Ephermal 256-Bit Curve 25519	Curve 25519 Key-pair
Key Derivation	HKDF	--	---
Verification of Correspondent Identity	✓	✓	✓ (Secret Chats)
Trust On First Use	✓	✕	✕
Self destruct messages	✕	✓	✓

5. discussion

The imperative features of WhatsApp, Viber and Telegram are compared in Table:1, and the comparison revealed that WhatsApp is the most eminent IM application due to its simple user interface and recognized security features in terms of E2EE and declared open-source code of its Signal protocol. Viber possesses its own proprietary protocol which is not declared publically but it is somewhat similar to Signal Protocol. Telegram is based on MTPro protocol which was initially subjected to security challenges but a modified version of MTPro after 2016 is fully secure even it has self-destructive feature of notification when a screenshot is taken by receiver. It provides security at two layers i.e. client-server and client-client.

6. conclusion and future directions

The importance of Instant Messaging applications cannot be denied in this recent age of technology. WhatsApp have successfully deployed all the security protocols and encryption techniques to make it secure application for its customers yet what about the privacy and security of metadata in the repository of WhatsApp that is still unencrypted. Although all the chats are fully encrypted yet WhatsApp do not provide facility of end to end encryption to backed up messages/media in google drive. Viber is no doubt providing quality of service to its customers but Viber code is not open to review and in case of “Key is stolen” past messages are not secure. With Telegram still there is a room for creating anonymous accounts, and experts declare that “home brewed and unproven cryptography” can lead to serious vulnerabilities as EFF (Electronic Frontier Foundation) provided 4/7 points on secure scorecard for chat function, 7/7 points for E2EE for secret chats.

On a concluding note, WhatsApp is most often used IM app due to its simple interface, Telegram provide better platform and Viber messenger is more serviceable.

Acknowledgment

I would like to thanks especially Dr. Ijaz Shaukat and Dr Muhammad Sheraz for guiding me throughout the research and paying special attention to my work.

References

[1] D. Marques et al., "Privacy and secrecy in ubiquitous text messaging," presented at the Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion, San Francisco, California, USA, 2012.

[2] J. Liu, Y. Fu, J. Ming, Y. Ren, L. Sun, and H. Xiong, "Effective and Real-time In-App Activity Analysis in Encrypted Internet Traffic Streams," presented at the Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, 2017.

[3] I. Del Pozo and M. Iturralde, "CI: A New Encryption Mechanism for Instant Messaging in Mobile Devices," Procedia Computer Science, vol. 63, pp. 533-538, 2015/01/01/ 2015.

[4] V. B. Liwandouw and A. D. Wowor, "The Existence Of Cryptography: A Study On Instant Messaging," Procedia Computer Science, vol. 124, pp. 721-727, 2017/01/01/ 2017.

[5] S. Schrittwieser et al., "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications," in NDSS, 2012.

[6] Y.-Y. Chen, F. Bentley, C. Holz, and C. Xu, "Sharing (and Discussing) the Moment: The Conversations that Occur Around Shared Mobile Media," presented at the Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services, Copenhagen, Denmark, 2015.

[7] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A critical review of 7 years of Mobile Device Forensics," Digital Investigation, vol. 10, no. 4, pp. 323-349, 2013/12/01/ 2013.

[8] A. Blanco-Justicia and J. Domingo-Ferrer, "Efficient privacy-preserving implicit authentication," Computer Communications, vol. 125, pp. 13-23, 2018/07/01/ 2018.

[9] M. Rahman, T. Akter, and A. Rahman, "Development of Cryptography-Based Secure Messaging System," J Telecommun Syst Manage, vol. 5, no. 142, pp. 2167-0919.1000142, 2016.

[10] W. Stallings, Cryptography and network security: principles and practice. Pearson Upper Saddle River, NJ, 2017.

[11] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, 2012, vol. 3, pp. 648-651: IEEE.
[12] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Journal of cryptology, vol. 26, no. 1, pp. 80-101, 2013.
[13] N. Unger et al., "SoK: secure messaging," in Security and Privacy (SP), 2015 IEEE Symposium on, 2015, pp. 232-249: IEEE.
[14] A. Herzberg and H. Leibowitz, "Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications," presented at the Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, Los Angeles, California, 2016.
[15] C. Baraniuk, "Phoney war," New Scientist, vol. 233, no. 3110, pp. 34-38, 2017.
[16] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A Formal Security Analysis of the Signal Messaging Protocol," in 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 2017, pp. 451-466.
[17] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," Computer Networks, vol. 102, pp. 83-95, 2016.
[18] E. Atwater and U. Hengartner, "Shatter: Using Threshold Cryptography to Protect Single Users with Multiple Devices," in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016, pp. 91-102: ACM.
[19] L. González-Manzano, J. M. d. Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, "PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things," Journal of Network and Computer Applications, vol. 71, pp. 59-71, 2016/08/01/ 2016.
[20] N. Unger and I. Goldberg, "Deniable Key Exchanges for Secure Messaging," presented at the Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, Colorado, USA, 2015.
[21] R. B. Lord, T. N. Hayes, and J. Uberti, "Secure instant messaging system," ed: Google Patents, 2018.
[22] Y. Li and Y. Wang, "Secure Electronic Transaction (SET protocol)," ed, 2014.
[23] A. De Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie, "Expert and non-expert attitudes towards (secure) instant messaging," in Symposium on Usable Privacy and Security (SOUPS), 2016.
[24] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, Viber and Telegram which is Best for Instant Messaging?," International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 3, pp. 909-914, 2016.
[25] S. Zimmeck et al., "Automated analysis of privacy requirements for mobile apps," in 24th Network & Distributed System Security Symposium (NDSS 2017), NDSS, 2017.
[26] R. E. Blahut, Cryptography and secure communication. Cambridge University Press, 2014.
[27] J. Buchmann, Introduction to cryptography. Springer Science & Business Media, 2013.
[28] S. Tully and Y. Mohanraj, "Chapter 2 - Mobile Security: A Practitioner's Perspective," in Mobile Security and PrivacyBoston: Syngress, 2017, pp. 5-55.
[29] N. Rastogi and J. Hendler, "WhatsApp security and role of metadata in preserving privacy," in ICMLG2017 5th International Conference on Management Leadership and Governance, 2017, p. 269: Academic Conferences and publishing limited.
[30] M. Bolli and P. Kofmel, "WhatsApp End-to-End Encryption."
[31] M. Sudozai, N. Habib, S. Saleem, and A. Khan, "Signatures of Viber Security Traffic," Journal of Digital Forensics, Security and Law, vol. 12, no. 2, p. 11, 2017.
[32] "Viber Encryption Overview."
[33] J. Job, V. Naresh, and K. Chandrasekaran, "A modified secure version of the Telegram protocol (MTProto)," in Electronics, Computing and Communication Technologies (CONECCT), 2015 IEEE International Conference on, 2015, pp. 1-6: IEEE.
[34] J. Jakobsen and C. Orlandi, "On the CCA (in)Security of MTProto," presented at the Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Vienna, Austria, 2016.

Nosheen Nazir was born in Chiniot, Punjab, Pakistan in 1992. She has completed her Graduation Degree in Information Technology from University of Sargodha, Punjab, Pakistan in 2015. She is currently a student of MS degree in Computer Science from the Riphah International University, Faisalabad, Pakistan.

In 2011, she received Prime Minister's based scholarship at Punjab College Chiniot, Punjab, Pakistan. In 2013, she secured 3rd Position all over the district in her under-graduation program. In 2014, she was selected for Prime Minister's Laptop Scheme for Youth of Pakistan and received a Laptop. In 2016, she passed a test from National Testing Service and stood 2nd in (Female) all over Chiniot, Punjab, Pakistan and she has been selected for Government Job in Education Department.

Her major areas of interest are Ecommerce, Marketing, Databases, Network Security, Machine Learning, Data Mining, and Data Warehousing.