Scientific Research Publishing

Journal of Information Security, 2018, 9, 95-99
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger

Robert E. Endeley

Capitol Technology University, Laurel, MD, USA
Email: reendeley@captechu.edu

How to cite this paper: Endeley, R.E. (2018) End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, **9**, 95-99.
https://doi.org/10.4236/jis.2018.91008

Received: December 22, 2017
Accepted: January 20, 2018
Published: January 23, 2018

Abstract

The ubiquity of instant messaging services on mobile devices and their use of end-to-end encryption in safeguarding the privacy of their users have become a concern for some governments. WhatsApp messaging service has emerged as the most popular messaging app on mobile devices today. It uses end-to-end encryption which makes government and secret services efforts to combat organized crime, terrorists, and child pornographers technically impossible. Governments would like a "backdoor" into such apps, to use in accessing messages and have emphasized that they will only use the "backdoor" if there is a credible threat to national security. Users of WhatsApp have however, argued against a "backdoor"; they claim a "backdoor" would not only be an infringement of their privacy, but that hackers could also take advantage of it. In light of this security and privacy conflict between the end users of WhatsApp and government's need to access messages in order to thwart potential terror attacks, this paper presents the advantages of maintaining E2EE in WhatsApp and why governments should not be allowed a "backdoor" to access users' messages. This research presents the benefits encryption has on consumer security and privacy, and also on the challenges it poses to public safety and national security.

Keywords

Instant Messaging, WhatsApp, End-to-End Encryption, National Security, Privacy

1. Introduction

The world is ever changing due to the advancement in the realm of science and technology, and these days it seems hard to escape the presence of technology in

our daily lives. Since Smartphones became popular, many messaging services have been launched. WhatsApp, which has more than 1.3 billion users in over 180 countries today, is a free messaging service owned by Facebook Inc., and has become more popular than others [1].

In 2009, Brian Acton and Jan Koum created WhatsApp purposely to make communication and the distribution of multimedia messaging easier and faster [2]. WhatsApp works with internet connectivity and helps its users to stay in touch with friends and relatives on their contact list. Apart from making its users get, and stay connected with each other, it also helps them to create groups, send images, videos, documents and audios [3].

As more and more people use WhatsApp as a means of communication, the importance of securing its users' business or private communications has become more imperative. Users of the app expect a reasonable amount of privacy for all their communications. To meet this expectation, WhatsApp in 2014 introduced End-to-End Encryption (E2EE) technology. This allows for data between communicating parties to be secure, free from eavesdropping, and hard to crack. This technology offers peace of mind to end users because their data are safe in transit, and third parties or even WhatsApp itself cannot access them; thus messages can only be decrypted by the recipient. While E2EE guarantees integrity, security, and privacy, it however, eliminates government surveillance and its ability to keep the country safe by intercepting terrorist communications.

2. Literature Review and Discussion

In light of this security and privacy conflict between the end users of WhatsApp and government's need to access messages in order to thwart potential terror attacks, this paper seeks to outline the advantages of maintaining E2EE in WhatsApp and why governments should not be allowed a "backdoor" to access users' messages.

Encryption is the scrambling of plaintext messages, turning it into unreadable code that can only be deciphered by those who have the secret key. End-to-End Encryption is one of the most commonly used technologies to secure and send information across the internet. Hardware embedded into phones and computers allows for the random locks and keys that make E2EE only work on the devices involved in the conversation. According to the [4], it is estimated that there were about 276 million internet users in the United States in 2014, and that number is predicted to rise. With this many users, the incentive for hackers to execute attacks and steal personal information increases.

According to a Javelin Strategy and Research Report in 2012, one in every four people who have a breach in their online data becomes a victim of identity theft as a result of that [5]. End-to-End Encryption provides an effective way to prevent these attacks, and if it had been implemented properly by Yahoo Inc., it could have prevented large-scale attacks like the one Yahoo suffered in 2016 and 2013, where almost 500 million, and more than 1 billion accounts were respectively compromised.

Governments, and secret services on the other hand are asking encrypted messaging services like WhatsApp to allow them access to their users' data [6]. There is growing risk to public safety as organized crime, terrorists, and child pornographers are drawn to the use of E2EE apps like WhatsApp that are technically impossible to access. According to [7], a defendant in a serious felony case told another individual on a recorded jailhouse call that "end-to-end encryption is another gift from God". Criminal defendants across the United States are benefiting from E2EE while the safety of all other American communities is in peril. However, providing a backdoor would not only be a breach of privacy to WhatsApp users, but creating a way for the authorities to read encrypted messages would also make the system vulnerable to cyber-attacks from criminals and other hackers.

By implementing backdoors, it also means that the service is not truly end-to-end encrypted in the first place. Microsoft Corporation created a backdoor into its popular messaging app Skype, even though its user base knew that Skype was fully endowed with end-to-end encryption technology. However, in 2013 government whistleblower Edward Snowden revealed that the platform did in fact, have a backdoor. This revelation led to a protest of Skype users and an eventual loss of credibility of the application. According to [8], in a response by Senator Ron Wyden regarding the US government's position in seeking encryption backdoor, the senator said in July 2017 that, "the US government does not need the approval of its secret surveillance court to ask a tech company to build an encryption backdoor". The implication is that the government can use its legal authority to secretly ask a US-based company for technical assistance, such as building an encryption backdoor into a product, but can petition the Foreign Intelligence Surveillance Court (FISC) to compel the company if it refuses.

Reference [9], reported a design feature in WhatsApp messaging service that could potentially allow some encrypted messages to be read by unintended recipients. WhatsApp allows undelivered messages to be stored in their servers for up to 30 days before they are deleted. Reference [9] noted that the WhatsApp implementation of the security protocol used in its E2EE allows for the generation of secret keys between communicating parties in a WhatsApp conversation. However, new keys get generated when a user gets a new phone or reinstalls WhatsApp. Messages for the user which may have been waiting to be delivered while the user was offline are then re-encrypted and resent automatically by the sender, without the sender having had an opportunity to verify whether the recipient is the person intended to receive the message. A sender is notified after the event if the sender has opted to turn on a notification in settings, but not otherwise. "This re-encryption and resending of previously undelivered messages could potentially allow a third party to intercept and read a user's undelivered messages in a situation where, for example, they had stolen a user's sim card. When the third party put the stolen sim card in another phone, they could then theoretically collect any messages that had not yet been delivered to the user in

question." [9]. WhatsApp Inc. has since responded to this claim, saying that the feature in question is a design tradeoff, meant to prevent users from losing their messages if they switch phones or reinstall the app.

3. Conclusion

While a majority of countries would favor some kind of restriction on access to unrecoverable encryption, there is no global consensus, and the likely outcome is a hodgepodge of national policies. According to [10], "Our research suggests that the risk to public safety created by encryption has not reached the level that justifies restrictions or design mandates". Lewis *et al.* further went on to say, "The encryption issue that law enforcement faces, while frustrating, is currently manageable". Communications privacy is a key element of human rights in the digital era, and developments affecting it ought to be reported. Ultimately, removing WhatsApp E2EE would not be the solution, as criminals could create their own, similar software that would allow them to communicate securely, while ordinary users would lose the ability to send genuinely private messages [6]. Maintaining E2EE in WhatsApp without an encryption backdoor guarantees genuine privacy in conversations between individuals and group chats. Voice conversations through WhatsApp messenger feel more natural; users are assured that no one is eavesdropping on their conversations, and conversations thus tend to feels more like a face-to-face conversation.

References

[1] Yeboah, J. and Ewur, G. (2014) The Impact of WhatsApp Messenger Usage on Students Performance in Tertiary Institutions in Ghana. *Journal of Education and Practice*, **5**, 157-164.

[2] Sarker, G.R. (2015) Impact of WhatsApp Messenger on the University Level Students: A Sociological Study. *International Journal of Natural and Social Sciences*, **2**, 118-125.

[3] Jisha, K. and Jebakumar (2014) A Trend Setter in Mobile Communication among Chennai Youth. *IOSR Journal of Humanities and Social Science* (*IOSR-JHSS*), **19**, 01-06.

[4] Central Intelligence Agency (2017) The World Factbook. Country Comparison, Internet Users. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html

[5] Pascual, A. (2013) Data Breaches Becoming a Treasure Trove for Fraudsters, 2013 Identity Fraud Report. https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters

[6] Michalas, A. (2017) How WhatsApp Encryption Works—And Why There Shouldn't Be a Backdoor. The Conversation. https://theconversation.com/how-whatsapp-encryption-works-and-why-there-shouldnt-be-a-backdoor-75266

[7] District Attorney New York County (2005) Going Dar: Encryption, Technology and the Balance between Public Safety and Privacy. District Attorney New York County,

Washington DC.

[8] Whittaker, Z. (2017) US Says It Doesn't Need Secret Court's Approval to Ask for Encryption Backdoors. http://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors

[9] Ganguly, M. (2017) WhatsApp Design Feature Means Some Encrypted Messages Could Be Read by Third Party. https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages

[10] Lewis, J., Zheng, D. and Carter, W. (2017) The Effect of Encryption on Lawful Access to Communications and Data. Center for Strategic & International Studies. A Report of the CSIS Technology Policy Program.