Like Intimate Secrets on a Postcard[1]

How Secure are Messaging Applications?

Theodore Tan
Fall 2016
Introduction to Computer Security

Mentor: Professor Ming Chow, Tufts University

[1] Naughton, John. "Your WhatsApp Secrets Are Safe Now. But Big Brother Is Still Watching You…." *The Guardian*. N.p., 10 Apr. 2016. Web. 01 Oct. 2016.

Abstract

Earlier this year, Facebook rolled out an end-to-end chat encryption feature for its Messenger service, the latest milestone in a trend towards tightening the security of messaging applications across the board. In recent times, there has been a much greater consumer demand for communication platforms to be secure, leading to both the modification of existing platforms and the creation of newer ones with more current security features. However, due to a variety of factors, security flaws still inevitably exist in many of these messaging platforms. This paper explores some of the current trends in making messaging more secure and the loopholes in these messaging platforms that have to be addressed in the near future.

* * *

Introduction

Currently, there seem to be two main, visible trends in the messaging application security landscape. Firstly, due to the increasing knowledge of the technology landscape, there is a heightened expectation from users for messaging apps to be more secure as well as a corresponding response by many developers to meet those expectations, even though some of them still fall short. Secondly, there have been increasing debate over the moral and legal implications of messaging app security, including if the government should have access to chat data, if complete encryption and security will allow messaging apps to be used for destructive purposes, etc. In this primarily user-targeted paper, the aim will be to tackle these issues and ultimately give users both a comprehensive overview of the state of

messaging app security as well as practical steps to ensure their personal security while choosing and/or using a messaging platform.

To The Community

In the words of Sherif Elsayed-Ali, Head of Amnesty International's Technology and Human Rights Team, "if you think instant messaging services are private, you are in for a big surprise. The reality is that our communications are under constant threat from cybercriminals and spying by state authorities. Young people, the most prolific sharers of personal details and photos over apps like Snapchat, are especially at risk."[2] His words emphasize a critical point – that is, in a world where privacy is increasingly important, the means by which we communicate are not always secure enough to maintain a privacy that many in our society today simply take for granted. A large percentage of our population use the services of some form of messaging application to communicate across the globe, and that is exactly why everyone should care. Not caring means allowing for unsafe practices to perpetuate, increasing the risk of security breaches, hacking, and other forms of attacks. On the other hand, taking the first step to be aware not only protects your own interests, but also forces software developers to be more conscious of the security and privacy choices they are making for their users.

[2] "Snapchat, Skype among Apps Not Protecting Users' Privacy." *News*. Amnesty International, 21 Oct. 2016. Web. 31 Oct. 2016.

The Current State of Security

At present, the most fundamental building block of messaging app security is end-to-end encryption (E2EE). Very simply, end-to-end encryption is "a way of transmitting a message so that it can only be read by the intended recipient, not being able to be intercepted by accessing the servers or the networks via which the message is sent." [3] When a conversation is initiated, the sender and recipient exchange unique cryptographic keys (generated by methods such as the pre-shared secret or the Diffie-Hellman key exchange) that are never stored as data and that even the software developers have no access to. Any message sent can only be decrypted upon receipt by the unique key, protecting against any spying, tapping, or attacks during the transport process. Due to the way the perception of security has evolved over the last few years, this layer of protection is almost an expected default for many users due to its importance and ease of implementation. A recent 2016 study by Amnesty International even slammed major platforms such as Snapchat, Microsoft's Skype, and Blackberry's Messenger for not adopting end-to-end encryption of its data, arguing that the "basic steps" of protecting the rights of the users were not even met.[4] This links back to the above-quoted words of Sherif Elsayed-Ali, as some of these extremely insecure applications are some of the most frequently used around the world – questioning just how aware users are about the security of the platforms they use on a daily basis.

Going one step further, the most secure messaging applications currently implement an additional layer of protection to protect their users. Signal, developed by Open Whisper Systems, is a prime example of such an application. It minimizes the data stored in its

[3] Macgoogan, Cara. "Revealed: The Most Secure Messaging Apps." *Technology*. The Telegraph, 25 Oct. 2016. Web. 31 Oct. 2016.
[4] Ibid.

databases, only storing information about the last time someone connected to its server and when a user signed up for signal, in order to reduce the possibility of metadata or other information being accessed from these databases.[5] In addition, Signal utilizes a system one of its original Lead Developers, Frederic Jacobs, describes as "anti-forensics architecture."[6] When users back up their phone to the cloud, Signal does not include any of its messages or the abovementioned encrypted database in the backup, effectively eliminating the risk of "accidentally handing over your private messages to any third-party company."[7] Due to this combination of security measures, any forensics done on a user's device will also yield extremely minimal results, as demonstrated by digital forensics and security expert Jonathan Zdziarski.[8]

This is in stark contrast with most of the messaging apps in the current market, in which such stringent security features are few and far between. Besides the blatantly unsafe apps that do not adopt end-to-end encryption, many of what we would consider to be the "safer" apps to currently use (such as Whatsapp, Telegram, Google Allo, etc) also have significant security loopholes. One of the issues is that many of these apps do not have a proper system to inform users if non-secure preferences are set by default or if non-secure practices are used in specific situations, such as when messages sent to non-iPhone users through iMessage are not encrypted.[9] As of October 2016, applications such as Facebook Messenger, Telegram, and Google Allo all did not have end-to-end encryption activated by

---

[5] Chen, Brian X. "Worried About the Privacy of Your Messages? Download Signal." *Personal Tech*. The New York Times, 07 Dec. 2016. Web. 11 Dec. 2016.
[6] Lee, Micah. "Battle of the Secure Messaging Apps: How Signal Beats Whatsapp." The Intercept, 22 June 2016. Web. 31 Oct. 2016.
[7] Ibid.
[8] Ibid.
[9] Clark, Liat. "WhatsApp Beats Telegram to Be Crowned the Most Secure Messaging App." *Security*. Wired, 25 Oct. 2016. Web. 31 Oct. 2016.

default (although Facebook's new "Secret Chat" feature is extremely secure) , needing users to take the extra step to turn on the preference or make some selection.[10] This easily translates into lapses in the security pipeline as users either forget or are lazy to change their preferences.

In addition, the architecture of many of the more secure apps still do not match up to Signal when subjected to a forensics test. In an article posted on his website, Zdziarski proves that while Whatsapp chats are end-to-end encrypted, forensic evidence of chats deleted from the application record are ever fully deleted from the database unless the entire app is wiped from the user's phone. This, he argues, is "common among any application that uses SQLite, because SQLite by default does not vacuum databases on iOS," and he cites Apple to have a similar problem with iMessage.[11] In a separate study, it was proven that Windows Instant Messaging apps such as Skype "can leave behind incriminating evidential material" when acquired and reconstructed as well.[12] It seems that in the current market, Signal is the only messaging app that has developed a truly anti-forensics architecture, which is somewhat surprising due to the fact that Signal's protocol is an open-source system.[13]

On a larger scale less pertinent to the individual user, a study by Robin Mueller revealed that malicious attackers can also make use of the insecure methods by which messaging apps conduct user authentication to obtain information about the wider user demographic of the application. These methods include authentication and account hijacking through phone number and SMS verification as well as manipulating how users upload their

[10] "Snapchat, Skype among Apps Not Protecting Users' Privacy." Amnesty International.
[11] Zdziarski, Jonathan. "WhatsApp Forensic Artifacts: Chats Aren't Being Deleted." Blog post. *Zdziarski's Blog of Things*. N.p., 28 July 2016. Web. 11 Dec. 2016.
[12] Yang, Teing Yee, et al. "Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies." *PLoS One* 11.3 (2016) *ProQuest.* Web. 29 Oct. 2016.
[13] Chen. "Worried About the Privacy of Your Messages? Download Signal." The New York Times.

phone book to the application server to enumerate through the server database and obtain user information or if a certain person is a user of the application.[14] Clearly, the security of messaging application architecture is not only crucial to protect each individual user, but also to protect the integrity of the application servers as well. These shortcomings then add up to present a current reality in which the security of messaging applications still has a long way to improve.

It is precisely in the context of talking about the positives and negatives of our electronic communication landscape that the moral discussion should be brought it. Can our information security and national security interests co-exist? In February 2016, Apple refused a court order to grant the FBI a brute force encryption backdoor to the iPhone of Syed Rizwan Farook, one of the shooters in the December 2015 San Bernardino massacre, asserting that the company "will continue to fight aggressively against requirements for companies to weaken the security of their systems."[15] This is just the latest incident in the struggle between governmental pressures to continually compromise the privacy of platform users in order to expedite issues of national concern, and the voices of many technology giants which all strongly back preserving the integrity of security systems and safeguards. Furthermore, in a world where terrorist groups such as ISIS are starting to use Telegram and self-developed encrypted Android apps to ensure communication privacy, this debate is sure to rage on in the near future as total encryption and privacy could hypothetically equip such groups with another tool for destructive purposes.[16] However,

---

[14] Mueller, Robin. "Security and Privacy of Smartphone Messaging Applications." *International Journal of Pervasive Computing and Communications*11.2 (2015): 132-50. Web. 31 Oct. 2016.
[15] Burgess, Matt. "Twitter and Facebook 'stand with' Apple in FBI Encryption Battle." *Technology*. Wired, 19 Feb. 2016. Web. 10 Dec. 2016.
[16] Alcorn, Chauncey L. "Here's What Tech ISIS Is Using to Spread Its Message." *Tech*. Fortune, 25 July 2016. Web. 10 Dec. 2016.

none of these reasons are fundamentally compelling enough to compromise the privacy that millions of users around the world deserve. The moral debate is extremely relevant and valid, but should never be an excuse for sub-par security development in the field.

Take Action: What Users Need to Know

With all these in mind, users of messaging apps must then ask themselves a very important question: Do I know how secure or insecure the app that I am using is and does it meet my needs? Due to the diverse range of applications currently on the market, ensuring one understands the possible vulnerabilities of a platform of choice is crucial in reducing ways in which information could be inadvertently compromised. This process could be broken down into three main questions:

Firstly, users should be aware of the nature of the material they are sending or receiving. Understandably, if a user is merely exchanging trivial information with another party, then perhaps any application would be a reasonable choice, so long as the user doesn't mind that conversation potentially being viewed by another party who could be screening or monitoring communication traffic. However, if sensitive information such as bank account numbers, passwords, or other personal details ae being exchanged, choosing an app that provides end-to-end encryption should be a bare minimum. Based on the analysis discussed in this paper, Signal should clearly be the applicable of choice as it leaves no forensic trace of correspondences on a user's device, ensuring that the information remains private. An even better option would just be to not trust the security of electronic communication and conduct that information exchange manually, if possible.

Secondly, users need to be aware of the default security settings of the application they are using, and know if they need to configure any setting to make their exchanges more secure. For example, both Whatsapp, Viber, Facebook Messanger, and Google Allo offer end-to-end encryption, although users have to manually choose certain options to activate it in the latter two cases. There is no compelling reason why developers choose to make a less secure configuration of their application as the default, but since that is the case, users need to be exceptionally vigilant in setting up their application environment to be the most secure one possible. Again, users need to be aware of the type of information they are sending, and what level of security is needed correspondingly.

Lastly, it is also useful to know how the application of choice handles backups of chat logs and application history. Although every application, with the exception of Signal, conceivably has some flaw in the security of this process, it is still important knowledge for the user to understand how the backend of the application works. With all this knowledge, users are then able to make an informed and comprehensive decision with regards to which application they are willing to utilize.

Conclusion

In a time when general security threats are clearly on the rise, as evidenced by some extremely recent high profile cases such as the public disclosure of Hilary Clinton's e-mails and the mass DDoS attack to DNS host Dyn in October 2016, we require greater electronic communication security and privacy more than ever. It is no longer sufficient to sit back and take security for granted. On the user end, a common reason why people resist upgrading to apps that afford greater privacy is because many of their friends or social circle do not yet

use those apps. If society as a whole is willing to recognize the threat poor privacy and security brings, request higher standards of security from developers, and move together safer options, that too would be a big step in increasing the privacy of all our communications. It is not only beneficial, but absolutely necessary, that we move towards demanding greater security in the applications we use so often in daily life.

Summary of References

Article References

Alcorn, Chauncey L. "Here's What Tech ISIS Is Using to Spread Its Message." *Tech*. Fortune, 25 July 2016. Web. 10 Dec. 2016.

Burgess, Matt. "Twitter and Facebook 'stand with' Apple in FBI Encryption Battle." *Technology*. Wired, 19 Feb. 2016. Web. 10 Dec. 2016.

Chen, Brian X. "Worried About the Privacy of Your Messages? Download Signal." *Personal Tech*. The New York Times, 07 Dec. 2016. Web. 11 Dec. 2016.

Clark, Liat. "WhatsApp Beats Telegram to Be Crowned the Most Secure Messaging App." *Security*. Wired, 25 Oct. 2016. Web. 31 Oct. 2016.

Lee, Micah. "Battle of the Secure Messaging Apps: How Signal Beats Whatsapp." The Intercept, 22 June 2016. Web. 31 Oct. 2016.

Macgoogan, Cara. "Revealed: The Most Secure Messaging Apps." *Technology*. The Telegraph, 25 Oct. 2016. Web. 31 Oct. 2016.

Naughton, John. "Your WhatsApp Secrets Are Safe Now. But Big Brother Is Still Watching You…." *The Guardian*. N.p., 10 Apr. 2016. Web. 01 Oct. 2016.

"Snapchat, Skype among Apps Not Protecting Users' Privacy." *News*. Amnesty International, 21 Oct. 2016. Web. 31 Oct. 2016.

Zdziarski, Jonathan. "WhatsApp Forensic Artifacts: Chats Aren't Being Deleted." Blog post. *Zdziarski's Blog of Things*. N.p., 28 July 2016. Web. 11 Dec. 2016.

Journal References

Mueller, Robin. "Security and Privacy of Smartphone Messaging Applications." *International Journal of Pervasive Computing and Communications*11.2 (2015): 132-50. Web. 31 Oct. 2016.

Yang, Teing Yee, et al. "Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies." *PLoS One* 11.3 (2016) *ProQuest.* Web. 29 Oct. 2016.