COMP 434
The Secure Messaging
Mustafa Saraç

From past to present, along with the techonological progress on the computer world, security became more of an issue for the humans and in today's world, this concern shows up as the secure messaging on the mobile communication applications, such as, Whatsapp, Signal and Telegram. As the smartphones take a great part in today's daily lives, most of the communication companies try to develop a solution by the worry of sensitive data transferring during conversations. The purpose of this paper is to discuss the advantages and disadvantages of mobile communication applications, in particular Whatsapp and Signal, comparatively.

Among the several applications that aim to provide security and privacy for the people, a few of them are distinguished by having some important security mechanisms which make more difficult to be abused by the adversary. As Cara McGoogan stated that Whatsapp is at the forefront of secure communication applications according to the research which was published by the Amnesty International and she adds that the reason of this leadership of Whatsapp is because they use end-to-end (E2E) encryption, which is an important security mechanism that guarantees other than the message sender and recipient, even Whatsapp itself cannot reach these sensitive messages (Telegraph 2016). In addition to end-to-end encryption, Samuel Gibbs explains that Whatsapp put into use the two-step verification mechanism in order to reduce the vulnerabilities of the system that an adversary might abuse (The Guardian 2017) In today’s world, these properties play a big role on improving the security level against possible attacks, so the companies like Whatsapp have the advantage of improved security level by having these properties in their system.

Signal, which is also one of the most popular secure communication applications, has end-to-end encryption and more security mechanisms when compared to the Whatspp. Micah Lee stated that Signal is an open source system which makes it safer than Whatsapp because of the reason that the system can be checked by security specialists against any vulnerability (The Intercept 2016) However, this is not possible for Whatsapp. In addition to this, Micah adds that Signal does not use any of the users’ messages during the backup process of third-party companies, such as Apple, so this advantage of Signal prevents the abuse of having sensitive messages, but Whatsapp adds these users’ messages to the backup files, which might be dangerous (The Intercept 2016). On the other hand, Signal will not have any chance to get back your chat history in case of any unwelcome situation such as changing the smartphone because of the reason that losing the old one according to the opinion of Micah (The Intercept 2016). As it is seen, Signal also has disadvantages right along with its advantages.

In conclusion, most of the communication companies tried to solve the security concern related to the messaging, in particular text messaging, by developing products with some security mechanisms, such as end-to-end encryption and two-step verification, during the recent years. Some of them, such as Whatsapp and Signal, get ahead of other applications by having different technologies in order to make it difficult to be affected by an adversary’s potential attack.

References

Telegraph 2016, *Revealed: The most secure messaging apps* **<http://www.telegraph.co.uk/technology/2016/10/25/revealed-the-most-secure-messaging-apps/ >.**

The Guardian 2017, *WhatsApp improves message security with two-step verification*
< https://www.theguardian.com/technology/2017/feb/10/whatsapp-improves-message-security-with-two-step-verification>.

The Intercept 2016, *Battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp*< **https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>.**