On the Development of Peer-to-Peer Decentralized Communication

Hilmar Gústafsson <hgusta16@student.aau.dk>

March 6, 2020

Abstract

We consider the problem of creating a peer-to-peer solution for decentralized communication.

1 Introduction

Internet chatting is an immensely popular activity. Recently, WhatsApp announced that they have 2 billion users [4]. Similarly, Facebook Messenger has announced having 1.3 billion users [3]. Both of these platforms require all participants in a conversation to have copies of the same software, i.e. WhatsApp or Facebook Messenger. But how safe are these platforms? Consider for example [1], a survey on different communication protocols. In terms of security, it is hard to verify the security of closed protocols. In addition, it is difficult to know what the owners of these proprietary protocols do with the data of their users. Additionally, having only one proprietary implementation means that all users are equally vulnerable to implementation-specific exploits. As recently as in 2019, it was reported that a private Israeli entity known as NSO Group has been targeting human-rights activists and journalists via this app [5].

Consider again the comparison in [1]. The highest rated protocol is Matrix [2], which is an open standard with various implementations.

References

[1] Digital communications protocols. https://docs.google.com/spreadsheets/d/1-UlA4-tslROBDS9IqHalWVztqZo7uxlCeKPQ-8uoFOU/edit#gid=0.

[2] Matrix.org. https://matrix.org.

[3] Messenger - more than 1.3 billion people. https://www.facebook.com/messenger/posts/1530169047102770.

[4] Whatsapp - two billion users - connecting the world privately. https://web.archive.org/web/20200215075032/https://blog.whatsapp.com/10000666/Two-Billion-Users--Connecting-the-World-Privately

[5] Whatsapp rushes to fix security flaw. https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html.