The Development of Peer-to-Peer Matrix

Hilmar Gústafsson <hgusta16@student.aau.dk>

March 10, 2020

Abstract

...

1 Introduction

Internet communication 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, respectively. Consider [7], a comparison of different communication protocols by Lance R. Vick in terms of security, privacy, compatibility and features.

Security Many of the features of the two mentioned examples cannot be verified, as they are propietary, closed-source software. It is hard to verify the security of closed protocols, and to know what the owners of these proprietary applications do with the data of their users. Having only one implementation means that all users are equally vulnerable to implementation-specific exploits.

Privacy Protocols which aren't decentralized force the users to trust the server on which the messages are stored. Even if the software is open source, there is no guarantee that it is the same software being run on the server without each user having read access to the server.

Compatibility Contrast this with the Simple Mail Transfer Protocol [6], which does not require the sender and the receiver to use the same software, but simply to implement the same standard. The former approach requires users to sign up for a service in order to communicate with others within that service, whereas the latter is naturally interoperable. We refer to this lack of interoperability as *the silo problem*.

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 WhatsApp [5]. Jeff Bezos, the founder of Amazon, was also reported to be the victim of a similar exploit [1]. The security of communication is important for many groups of people, whose livelihood or lives may depend on it. The journalists and human-rights activists might, for example, require anonymous communication to stay safe from hostile governments, or institutions. Take for example the Saudi Arabian government, which has been accused of assassinating journalists [2]. It could also be in the interest of companies to have platforms for communication within the company, in order to reduce the chances of exploits infecting company hardware. For private citizens, the security and privacy of their conversations on the internet may be important to them for many reasons, and recent changes in law reflects the stance that governments take against corporations who may wish to violate the privacy of their users.

1.1 Initial Problem Statement

One of the solutions for *the silo problem* is to establish an open standard which can be implemented freely by individual parties. Given that this standard is implemented correctly, the different implementations are interoperable.

We propose the following initial problem statement:

- What are the properties of a good solution to *the silo problem*?
- How can the existing protocols in [7] be improved with regard to these properties?

2 Analysis

We explore the different questions posed in the initial problem statement in section 1.1

2.1 The Silo Problem

The Silo problem is...

2.2 Problem Statement

- What are the architectural consequences and trade-offs in peer-to-peer communication?
- What are the properties of a good solution?
- How could one implement such a solution?

References

[1] How jeff bezos' iphone x was hacked. https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html. Last accessed: March 6th, 2020.

[2] Khashoggi killing: Un human rights expert says saudi arabia is responsible for "premeditated execution". https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24713&LangID=E. Last accessed: March 7th, 2020.

[3] Messenger - more than 1.3 billion people. https://www.facebook.com/messenger/posts/1530169047102770. Last accessed: March 6th, 2020.

[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. Last accessed: March 6th, 2020.

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

[6] J. Klensin. Simple mail transfer protocol. RFC 5321, RFC Editor, October 2008. http://www.rfc-editor.org/rfc/rfc5321.txt.

[7] Lance R. Vick. Lance r. vick on twitter: "i finally started a spreadsheet to compare relative security, privacy, compatibility, and features of various messenger systems. tl;dr @riotchat / @matrixdotorg is winning on all fronts. https://t.co/7zxczdjwwj" / twitter. https://twitter.com/lrvick/status/1051260991479013376, 2018. Last accessed: March 7th, 2020.