Decentralised Social Media: Protecting Privacy of Vulnerable Communities – Design Fiction

Dorota Filipczuk
Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
dorota@ecs.soton.ac.uk

m.c. schraefel
Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
mc@ecs.soton.ac.uk

ABSTRACT

This paper is presented as a "design fiction" describing a decentralised social media platform protecting privacy of vulnerable user groups in the world where all server-client communication is public. We consider possible impact of the tool on privacy and security of the users by presenting fictional findings from field studies.

1. INTRODUCTION

Upon enforcement of new legal regulations around the world, the Internet companies decided to open-source their databases. All of a sudden, personal information stored in the corporate data centers was suddenly made public. Over the months, the majority of users got used to the fact that everyone can read their emails, access backups of their documents and check their bank account balance. However, to vulnerable groups such as people living in countries where freedom of speech is not exercised, public figures whose relationships are under constant attention of mainstream media and in particular, and activists campaigning against the regulation, this event caused a significant exclusion from any kind of online communication. Often living far away from their families, privacy and security are at risk when using social media platforms.

Researchers have looked into ways of applying currently existing solutions to this problem. Blockchain technology [4] provides a way of decentralising data, however security of identity in this peer-to-peer communication system has previously been questioned [5]. Other decentralised data sharing systems such as the Solid project [1] and the WebBox [6] assume that users will either host their own servers, which requires technical skills, or rent cloud servers run by other companies or organisations, which may not be ideal when trust plays a role.

The rapid pace of hardware advances in both the speed and capacity of storage devices, as well as bandwidth, make it possible to exchange large quantities of data directly between portable, personal devices such as laptops and mobile phones. We present a tool based on this assumption.

2. METHOD

PrivateSM is a decentralised social media platform that follows the unhosted web app principles [3, 2]. As opposed to the popular client-server architectures, this peer-to-peer communication system does not send user data to its servers. Instead, it is stored on their own devices, encrypted end-to-end. Users can broadcast posts to all of their contacts and send private messages to one or more users. The messaging protocol allows full user control over each individual piece of data – when the data (a text message, post, photo etc.) is sent to another device, it is still linked to the sender if they wish to modify it. The data format also contains an expiration date (set by the sender), after which it disappears from all devices storing it.

We evaluated the platform with participants from the vulnerable communities and well as other people who they wanted to keep in touch with, including their family members and friends. As part of our field study, the participants were instructed to use PrivateSM and write journals for 90 days, where they describe their communication and feelings daily.

3. RESULTS

We analysed the journals, looking for common themes. We initially noticed a huge excitement about this new technology – both the vulnerable groups, and their families and friends were happy that they can finally communicate without a fear of being eavesdropped or tracked down. The majority of users expressed feeling in control of their data. Storing data on their phones was convinient when they had to change location (P1: "*I now travel with my data*").

However, we found that the aspects of the system that were supposed to protect users, also introduced new issues. A common problem identified was related to security of the people from the vulnerable groups, and inability to track their location when a user was not responding (P2: "*I don't know what she's up to, maybe something happened... can't check where [she] is, if [she] spoke with anyone...*"). A couple of the participants had concerns about no central authority being control over the content published (P3: "*He doesn't want to delete that picture and I have no one to report it to!*"). There is no way of inferring users' traits by the system, and no way of telling whether a person is trustworthy (P4: "*I don't know if that friend of her is a good guy*"). Few of the participants reported mistrust of the system (P5: "*How do I know that no one is reading my messages?*"; P6: "*Not sure if the person I'm talking to is really my brother or someone else*").

4. CONCLUSION

In this "design fiction", we use an imaginary example of a social media tool, where information is *not* stored on servers, but on personal devices. We conclude that although this approach solves certain problems, it creates new ones that need to be taken into account when designing privacy technology for vulnerable communities.

5. REFERENCES

[1] Solid. https://solid.mit.edu/. Accessed on 17 May 2019.

[2] Unhosted - building web apps without servers | scott's workblog. https://scottbw.wordpress.com/2012/08/29/unhosted-building-web-apps-without-servers/. Accessed on 17 May 2019.

[3] unhosted web apps. https://unhosted.org/. Accessed on 17 May 2019.

[4] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[5] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[6] D. A. Smith, M. Van Kleek, O. Seneviratne, m. c. schraefel, R. Bertails, T. Berners-lee, W. Hall, and N. Shadbolt. Webbox: Supporting decentralised and privacy-respecting micro-sharing with existing web standards. 2012.