Building Blocks for Privacy-Preserving Decentralized OSNs

Daniel Bosk, Sonja Buchegger, Benjamin Greschbach, and Guillermo Rodríguez-Cano

School of Computer Science and Communication
KTH Royal Institute of Technology
Stockholm (Sweden)

(Contact: gurc@csc.kth.se)

Nowadays, there is more data stored in online services than ever, mainly because of the widespread use of the Internet and the maturing of communication technologies, but also due to the popularization of Online Social Networks (OSNs).

Most of these services are run in a centralized manner such that the provider of the service acts as the communication channel between the users. Being such a hub allows the providers to oversee a large amount of information, and in the case of OSNs, much of it of a personal and sensitive kind, e.g., life events, geo-located pictures or simply professional life.

OSNs have an unfortunate and controversial history of privacy issues, e.g., accidental and intentional data leakages, and security problems, e.g., censorship, discrimination. Such dependence on the provider has gained relevance, and become a great concern for the general population in the recent years, especially after the news of the global mass surveillance program by the United States National Security Agency in collaboration with some of these providers and other governmental intelligence agencies.

Users are fairly aware of the business model supporting, improving and maintaining these systems, i.e., advertisement or customer profiling. However, these business models also create an incentive to keep collecting and mining more data, and a disincentive to protect the privacy of the user.

For such highly connected data-intensive services we propose a shift to decentralized and privacy-preserving solutions where users can have full control over their data. Decentralized to reach provider independence, and privacy-preserving to provide data protection by prevention, i.e., by cryptographic means and access control.

Our proposal of a privacy-preserving decentralized OSN aims at implementing current functionality present in modern OSNs with privacy-preserving properties and exploring what other features can be implemented in such decentralized scenario. We also analyze the trade-offs that have to be made in terms of meta-data inferences, heterogeneity, availability, scalability, robustness and efficiency.

We have designed some important building blocks: access control by applying a policy-hiding cryptographic scheme, usable password authentication in P2P networks, targeted user search by means of user defined knowledge threshold, and events coordination mechanism without the need of a trusted third party. Currently, we are investigating the implications of aggregating the friend-activity feed, the scheduling of events in a privacy-preserving manner, and other efficient access control alternatives in our decentralized setting.

Acknowledgements
Portions of this work have been done in collaboration with Oleksandr Bodriagov (obo@csc.kth.se) and Gunnar Kreitz (gkreitz@csc.kth.se) while they were at KTH Royal Institute of Technology.
This research has been funded by the Swedish Foundation for Strategic Research grant SSF FFL09-0086 and the Swedish Research Council grant VR 2009-3793.