Privacy in Decentralized Online Social Networks: Metadata Issues and Adversary Models

Benjamin Greschbach

May 2, 2012

As people use Social Network Services (SNS) to organise their social life, privacy issues are an inherent concern in these services. Currently, a user must trust the SNS provider to enforce access rights, not to misuse the provided content, and to be sufficiently secured against third-party attacks. For today's popular SNS providers, however, it is said that people are not customers, but primarily products. The business model of these services is based on targeted advertisements, and they have an infamous history of data leakages and privacy breaches.

Decentralised Online Social Networks (DOSN) are evolving as a promising response to these shortcomings. The decentralization has the potential to mitigate design-inherent privacy flaws of logically centralized services such as Facebook, Google+ or Twitter. A common approach to build a DOSN is to use a peer-to-peer (P2P) architecture. Recruiting the participants for data management and communication processing is not only beneficial from the privacy perspective but is also advantageous for the resilience and scalability of a system.

Access control for published content is enforced by cryptographic means so that users need not rely on policies or the goodwill of a central provider. In addition, users keep the physical ownership of their content, which prevents censorship, yields higher resilience with respect to network outages, and facilitates data portability.

While the absence of a single point of data aggregation strikes the most powerful attacker from the list of adversaries, the decentralization also removes some privacy protection afforded by the central party's intermediation of all communication. As content storage, access right management, retrieval and other administrative tasks of the service become the obligation of the users, it is non-trivial to hide the metadata of objects and information flows, even when the content itself is encrypted. Such metadata is, deliberately or as a side effect, hidden by the provider in a centralized system.

Furthermore, new adversaries enter the stage when SNS data is spread out in a P2P network, that exhibits more diverse points of attack. One of several adversary models, that become more relevant in the decentralized setting, is that of a friend adversary: an attacker that exploits the social relationship status established to the target user. Together with background knowledge, possibly acquired outside the SNS, this adversary can mount powerful inference attacks.

I will present previous and ongoing work on identifying the privacy challenges that arise, once a centralized SNS is replaced by a DOSN. This comprises a systematic discussion of possible privacy breaches, stemming not from the content itself but from its metadata (like size or structure) or data handling (such as communication flows). Furthermore, this includes the analysis of the different adversary models, relevant for a DOSN environment. Finally, I summarize approaches to mitigate these problems, including those suggested by proposed DOSN implementations.