Social Graph based Access Control Policies in Decentralized Online Social Networks

Benjamin Greschbach, KTH Stockholm

May 12, 2015

In the context of an Online Social Network (OSN), access control can leverage the information contained in the social graph to allow for access control policies beyond explicitly granting access to a known audience. One example are friend-of-a-friend policies, where a user states that access to some information should be granted to her friends, and their friends, without the user having a direct relation to these friends of her friends. Implementing this functionality in a privacy-preserving Decentralized Online Social Network (DOSN) is a challenge because the social graph information is private, e. g., a user should not learn the complete list of friends of a friend.

In previous work, we have designed a basic event invitation feature for DOSNs. It allows users to invite other users for an event and discloses related information such as how many people are invited, how many committed to attend, or some private details about the event to a specified audience such as only invited users or only attending users.

In our ongoing work, we want to explore the possibilities to extend the event invitation feature leveraging social graph information. Invited users could for example be allowed to pass on an invitation to their friends, but not further (or more general, only a fixed number of hops in the social graph). Another type of social graph information possible to use is the time when friendship relations have been established. An organizer of an event might for example restrict the transfer of invitations to those users that have been friends of her friends for a certain amount of time, avoiding the ad-hoc friendship establishment in order bypass the restrictions.

One use case example for this feature is the context of activists engaged in political dissent, being worried about the infiltration by undercover state authority agents. The activists might be organized in a loose network, where not everybody personally knows each other, but some transitivity of trust relations is assumed. When organizing a political gathering they might want to make use of this invitation feature in order to spread the invitation to a wider audience while at the same time reduce the risk of incautious users leaking it to newly established, and therefore potentially dangerous contacts.

In this work we want to explore how social graph information such as existence and establishing-time of friendship relations can be used for access control policies in a decentralized system, while at the same time protecting the privacy of the users with respect to this information.

For the friend-of-a-friend policy schemes, we will look at blind signature schemes and anonymous credentials, to see how they can be adapted for this purpose.

For the establishing-time based policy schemes, we will look at decentralized write-once techniques such as Merkle hash trees or proof-of-work based block chains as in the Bitcoin architecture, that can store an unforgeable and time-stamped history of friendship establishments. As these datastructures are public by design, the friendship relation information has to be stored in a confidential, but provable way. For this purpose we will try to adapt non-interactive zero-knowledge proof schemes or cryptographic hash based techniques. A simple approach would be for example to let the two users that establish a friendship relation, each sign each other's public keys, then hash these signatures together with a random number chosen by the two users and store the resulting hash value in the write-once datastructure. In this way, the published data does not reveal anything about the friendship relation while the two users can later on convince a third party that they have been friends at least since this entry was written (e. g., by providing the two signatures, the random number and a pointer to where in the write-once datastructure the entry is located).