User search is one fundamental functionality of an Online Social Network (OSN). When building privacy-preserving Decentralized Online Social Networks (DOSNs), the challenge of protecting user data and making users findable at the same time has to be met. We propose a user-defined knowledge threshold (“find me if you know enough about me”) to balance the two requirements. We suggest, discuss and evaluate two decentralized protocols for this purpose.

Popular OSNs are logically centralized systems. The massive information aggregation at the central provider inherently threatens user-privacy. Data leakages, whether intentional (e.g., selling of user data to third parties) or unintentional (e.g., by attacks from outsiders), happen regularly. Motivated by these insights, decentralization has been proposed to mitigate these threats. When decentralizing a system, two challenges have to be met: to implement equal functionality without centralized components, and to provide user privacy under a significantly different threat model.

Here, we look at the functionality of user search, i.e., the lookup of a system-specific user identifier (e.g., a URI of a profile) based on information about the user (e.g., name, city, affiliation). The ability to search for users, in conjunction with other ways of traversing the social graph (e.g., friendlist of friends), is a basic building block of an OSN that allows users to find each other and thereby establish links.

We propose two protocols to support user search in a DOSN that shield user data from searchers who know less than a user-specified threshold amount of information about the target. To our knowledge, this consideration is a novel form of knowledge-based access control. This type of restriction was inspired by an observation by Fong et al. (2009) that being able to reach a user in an OSN is an integral part of access control in such systems.

We evaluate our protocols using real world data from the U.S. census to relate the performance for legitimate users to the brute-force costs of an adversary. The latter depend on the user defined knowledge threshold and the knowledge of the adversary about the target user. The results suggest that for common attributes, the proposed protocols offer promising protection against an adversary that knows at least two or three attributes less than required by the user.