Encryption for Peer-to-Peer Social Networks

Oleksandr Bodriagov
School of Computer Science and Communication
KTH - Royal Institute of Technology
obo@kth.se

Abstract

To address privacy concerns over online social networking services, several decentralized alternatives have been proposed. These peer-to-peer (P2P) online social networks do not rely on centralized storage of user data. Rather, data can be stored not only on a profile owner's computer but almost anywhere (friends' computers, random peers from the social network, third-party external storage, etc.). Because external storage is often untrusted or only semi-trusted, encryption plays a fundamental role in the security of P2P social networks.

Encryption, however, also adds some overhead in both the time and space domains. To be scalable, a system that relies heavily on encryption should use as efficient algorithms as possible. It also needs to provide the functionality of changing access rights at reasonable cost, and, crucially, the system should preserve privacy properties itself. That is, beyond user data confidentiality, it has to protect against information leakage about users' access rights and traffic analysis.

We explored the encryption requirements for P2P social networks and proposed a list of evaluation criteria that we use to compare existing approaches. We have found that none of the current P2P architectures for social networks achieve secure, efficient, 24/7 access control enforcement and data storage. They rely on trust, require constantly running servers for each user, use expensive encryption, or fail to protect the privacy of access information. In a search for solutions that better fulfill our criteria, we found that some broadcast encryption (BE) and predicate encryption (PE) schemes exhibit several desirable properties.

We make measurements to evaluate encryption/decryption speed of the PE schemes. If encryption/decryption operations take reasonable time (from the usability perspective), then the corresponding scheme should be considered as a quite suitable candidate for P2P social networks' encryption. Eventually, the aim is to describe how typical operations of social networks are performed in the decentralized setting using a PE or a BE scheme and simulate these operations.

Keywords: P2P social network, encryption-based access control, broadcast encryption, predicate encryption