Privacy-Preserving Access Control in Decentralized Online Social Networks using Anonymous Broadcast Encryption

Daniel Bosk and Sonja Buchegger

School of Computer Science and Communication
KTH Royal Institute of Technology, Stockholm, Sweden
Email: {dbosk,buc}@kth.se

Online social networks collect and store large amounts of private data. Trusting too much data with third parties is a privacy risk. For this reason distributed online social networks (DOSNs) was proposed. Among the benefits of DOSNs are that users can keep control of their data, there is no central provider through which third parties (by force) can access it, and it is more difficult to censor. However, these require more research to ensure security and privacy, as the decentralized structure opens up for other risks—even when data is encrypted.

The current research on access control in DOSNs has focused on efficiently achieving confidentiality for data. Although the data receives privacy, the access-control structures and patterns do not. We focus on achieving efficient privacy-preserving access control mechanisms for the DOSN setting, i.e. hidden policies, hidden credentials and hidden decisions.

We use the DOSN setting to adapt anonymous broadcast encryption for better performance. There are some properties of the underlying distributed storage structure which can be utilized for better efficiency and privacy properties. However, there is usually a trade-off between privacy and efficiency. In this work we evaluate the privacy properties and the complexity of different trade-offs. One trade-off we explore is to use the push model for a replacement of the storage expensive anonymous tag-hint system suggested for anonymous broadcast encryption. This way a subscriber knows which ciphertext is meant for her, since all ciphertexts pushed to her inbox are for her. This has the further advantage of hiding the size of the recipient set.

Another trade-off investigated is to use a semantically secure symmetric cipher instead of an IND-CCA2 public-key encryption. The original anonymous broadcast encryption scheme was constructed for an IND-CCA2 public-key encryption scheme, but to scale better for DOSNs we look into using a less computationally complex scheme, like a semantically secure symmetric cipher.

There are also other problems to consider. For example, broadcast encryption was designed to broadcast a message to a dynamically changing group. As such, changing access policies for already existing objects requires only one re-encryption of the object and a re-broadcast to the new set of authorized subjects. This requires the subjects to keep track of those keys. On the other hand, binding many objects to the same key results in the need for re-encryption of many objects in the case of a change of policy.