Cryptography for peer-to-peer online social media

Ruben De Smet

Vrije Universiteit Brussel, Belgium

(Joint work with Ann Dooms, Jo Pierson)

Online social media are often criticised for their lack of *institutional* privacy: they mine users' data, and make a profit by selling profiles. By encrypting the data, those companies can no longer access them; however, this also takes out the incentive to host the platform and data for its users. Peer-to-peer networks do not rely on a central institute to host data; instead, users' devices host data for each other.

Peer-to-peer networks however come with a problem of their own: no single node can be trusted, which may infringe the users' *social* privacy. Many solutions have been proposed, often complicating the (already complicated) development process of the system. These systems draft a new protocol on a per-feature basis, requiring the developer to think about cryptography, key management and network protocols. This is in contrast with the development of centralised counterparts, where the developer can focus on the content of the application.

We take a first step to build a generic peer-to-peer *platform*, on top of which online social media applications can be developed. By abstracting over the cryptography and the network components, we alleviate the work of the developer. The platform is based on a graph database model, which is only efficiently queryable by legitimate users.

Vrije Universiteit Brussel, Campus Etterbeek, 1050 Brussel, Belgium
rubedesm@vub.ac.be