Cryptology ePrint Archive: Report 2011/640

Hummingbird: Privacy at the time of Twitter

Emiliano De Cristofaro, Claudio Soriente, Gene Tsudik, Andrew Williams

Abstract: In the last several years, micro-blogging Online Social Networks (OSNs), such as Twitter, have taken the world by storm, now boasting over 100 million subscribers. As an unparalleled stage for an enormous audience, they offer fast and reliable centralized diffusion of pithy tweets to great multitudes of information-hungry and always-connected followers. At the same time, this information gathering and dissemination paradigm prompts some important privacy concerns about relationships between tweeters, followers and interests of the latter. In this paper, we assess privacy in today's Twitter-like OSNs and describe an architecture and a trial implementation of a privacy-preserving service called Hummingbird. It is essentially a variant of Twitter that protects tweet contents, hashtags and follower interests from the (potentially) prying eyes of the centralized server. We argue that, although inherently limited by Twitter's mission of scalable information-sharing, this degree of privacy is valuable. We demonstrate, via a working prototype, that Hummingbird's additional costs are tolerably low. We also sketch out some viable enhancements that might offer better privacy in the long term.

Category / Keywords: privacy micro-blogging OSN multi-party computation

Publication Info: To appear in IEEE Symposium on Security and Privacy (SP 2012)

Date: received 28 Nov 2011, last revised 5 Mar 2012

Contact author: edc at parc com