Cryptology ePrint Archive: Report 2011/026

Private Discovery of Common Social Contacts

Emiliano De Cristofaro and Mark Manulis and Bertram Poettering

Abstract: The increasing use of computing devices for social interactions fuels the proliferation of online social applications, yet prompts a number of privacy concerns. One common problem occurs when two unfamiliar users, in the process of establishing social relationships, want to assess their social proximity by discovering mutual social contacts.

In this paper, we introduce \emph{Private Contact Discovery}, a novel cryptographic primitive that lets two users, on input their respective contact lists, learn their common contacts (if any), and nothing else.

We present an efficient and provably secure construction, that (i) prevents arbitrary list manipulation by means of contact certification, and (ii) guarantees user authentication and revocability. Following a rigorous cryptographic treatment of the problem, we define \emph{contact-hiding} security and prove it for our solution, under the RSA assumption in the Random Oracle Model (ROM). We also show that other related cryptographic techniques are unsuitable in this context. Experimental analysis on various types of devices attests to the practicality of our technique, which achieves computational and communication overhead almost linear in the number of contacts.

Category / Keywords: cryptographic protocols / private contact discovery, contact-hiding, IHME, social networks

Publication Info: A preliminary version of this paper appears in the Proceedings of ACNS 2011.

Date: received 12 Jan 2011, last revised 14 Apr 2011

Contact author: edecrist at uci edu; mark at manulis eu; bertram poettering at cased de