Cryptology ePrint Archive: Report 2011/064

Cryptographic Treatment of Private User Profiles

Felix Günther and Mark Manulis and Thorsten Strufe

Abstract: The publication of private data in user profiles in a both secure and private way is a rising problem and of special interest in, e.g., online social networks that become more and more popular. Current approaches, especially for decentralized networks, often do not address this issue or impose large storage overhead. In this paper, we present a cryptographic approach to \emph{private profile management} that is seen as a building block for applications in which users maintain their own profiles, publish and retrieve data, and authorize other users to access different portions of data in their profiles. In this course, we provide: (i) formalization of \emph{confidentiality} and \empf{unlinkability} as two main security and privacy goals for the data which is kept in profiles and users who are authorized to retrieve this data, and (ii) specification, analysis, and comparison of two private profile management schemes based on different encryption techniques.

Category / Keywords: cryptographic protocols / private user profiles, social networks, privacy, access control

Publication Info: A preliminary version of this paper appears in Proceedings of FC 2011 / RLCPS Workshop. This is the full version.

Date: received 3 Feb 2011

Contact author: mark at manulis eu

Available formats: PDF | BibTeX Citation

Version: 20110208:131701 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]