Cryptology ePrint Archive: Report 2011/041

Reclaiming Privacy for Smartphone Applications (Revised Version)

Imad Aad and Emiliano De Cristofaro and Anthony Durussel

Abstract: The scope of mobile phones has skyrocketed in recent years to such an extent that smartphone sales are expected to surpass those of PCs by the end of 2011. Equipped with relatively powerful processors and fairly large memory and storage capabilities, smartphones can accommodate increasingly complex interactive applications. As a result, the growing amount of sensitive information shared by smartphone users raises serious privacy concerns and motivates the need for appropriate privacy-preserving mechanisms. In this paper, we present a novel architecture geared for privacy-sensitive applications where personal information is shared among users and decisions are made based on given optimization criteria. Specifically, we focus on two application scenarios: (i) privacy-preserving interest sharing, i.e., discovering shared interests without leaking users' private information, and (ii) private scheduling, i.e., determining common availabilities and location preferences that minimize associate costs, without exposing any sensitive information. We propose efficient yet provably-private solutions, and conduct an extensive experimental analysis that attests to the practicality of the attained privacy features.

Category / Keywords: cryptographic protocols / privacy, multi-party computation

Publication Info: A preliminary version of this paper appears in the Proceedings of IEEE PerCom 2011

Date: received 21 Jan 2011, last revised 9 Nov 2011

Contact author: edecrist at uci edu

Note: This version adds Section 4.3.3 to further discuss how the PrivSched-v2 algorithm trades off some privacy guarantees with increased efficiency.