Cryptology ePrint Archive: Report 2011/113

Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information

Emiliano De Cristofaro and Yanbin Lu and Gene Tsudik

Abstract: The need for controlled (privacy-preserving) sharing of sensitive information occurs in many different and realistic everyday scenarios, ranging from national security to social networking. We consider two interacting parties, at least one of which seeks information from the other: the latter is either willing, or compelled, to share information. This poses two challenges: (1) how to enable this type of sharing such that parties learn no information beyond what they are entitled to, and (2) how to do so efficiently, in real-world practical terms. This paper explores the notion of Privacy-Preserving Sharing of Sensitive Information (PPSSI), and provides two concrete and efficient instantiations, modeled in the context of simple database querying. Proposed techniques function as a privacy shield to protect parties from disclosing more than the required minimum of their respective sensitive information. PPSSI deployment prompts several challenges, that are addressed in this paper. Extensive experimental results attest to the practicality of attained privacy features and show that they incur quite low overhead (e.g., 10% slower than standard MySQL).

Category / Keywords: cryptographic protocols /

Date: received 7 Mar 2011, last revised 18 Apr 2011

Contact author: edecrist at uci edu