Cryptology ePrint Archive: Report 2011/235

Computer-Aided Decision-Making with Trust Relations and Trust Domains (Cryptographic Applications)

Simon Kramer and Rajeev Goré and Eiji Okamoto

Abstract: We propose generic declarative definitions of individual and collective trust relations between interacting agents and agent collections, and trust domains of trust-related agents in distributed systems. Our definitions yield (1) (in)compatibility, implicational, and transitivity results for trust relationships, including a Datalog-implementability result for their logical structure; (2) computational complexity results for deciding potential and actual trust relationships and membership in trust domains; (3) a positive (negative) compositionality result for strong (weak) trust domains; (4) a computational design pattern for building up strong trust domains; and (5) a negative scalability result for trust domains in general. We instantiate our generic trust concepts in five major cryptographic applications of trust, namely: Access Control, Trusted Third Parties, the Web of Trust, Public-Key Infrastructures, and Identity-Based Cryptography. We also show that accountability induces trust. Our defining principle for weak and strong trust (domains) is (common) belief in and (common) knowledge of agent correctness, respectively.

Category / Keywords: foundations / cryptographic-key management; TTP; Web of Trust; PKI

Publication Info: see corresponding footnote on first page

Date: received 12 May 2011, last revised 22 Mar 2012

Contact author: simon kramer at a3 epfl ch