Data Usage Control for Distributed Systems

Abstract:
Data usage control enables data owners to enforce policies over how their data may be used after it has been released and accessed. We address distributed aspects of this problem, which arise if the protected data resides within multiple systems. We contribute by formalizing, implementing, and evaluating a fully decentralized system that (i) generically and transparently tracks protected data across systems, (ii) propagates data usage policies along, and (iii) efficiently and preventively enforces policies in a decentralized manner. The evaluation shows that (i) data flow tracking and policy propagation achieve a throughput of 21%–54% of native execution, and (ii) decentralized policy enforcement outperforms a centralized approach in many situations.

Stichworte:
Security and privacy: Information accountability and usage control; Formal security models; Access control; Digital rights management