Privacy-Preserving Network Provenance

Adam O'Neill, University of Massachusetts Amherst

Network accountability, forensic analysis, and failure diagnosis are becoming increasingly important for network management and security. Network provenance significantly aids network administrators in these tasks by explaining system behavior and revealing the dependencies between system states. Although resourceful, network provenance can sometimes be too rich, revealing potentially sensitive information that was involved in system execution. In this paper, we propose a cryptographic approach to preserve the confidentiality of provenance (sub)graphs while allowing users to query and access the parts of the graph for which they are authorized. Our proposed solution is a novel application of searchable symmetric encryption (SSE) and more generally structured encryption (SE). Our SE-enabled provenance system allows a node to enforce access control policies over its provenance data even after the data has been shipped to remote nodes (e.g., for optimization purposes). We present a prototype of our design and demonstrate its practicality, scalability, and efficiency for both provenance maintenance and querying.