Capecchi, Sara; Castellani, Ilaria; Dezani-Ciancaglini, Mariangiola

Typing access control and secure information flow in sessions. (English) [Zbl 1360.68207]

Summary: We consider a calculus for multiparty sessions with delegation, enriched with security levels for session participants and data. We propose a type system that guarantees both session safety and a form of access control. Moreover, this type system ensures secure information flow, including controlled forms of declassification. In particular, it prevents information leaks due to the specific control constructs of the calculus, such as session opening, selection, branching and delegation. We illustrate the use of our type system with a number of examples, which reveal an interesting interplay between the constraints of security type systems and those used in session types to ensure properties like communication safety and session fidelity.

MSC:
68M14 Distributed systems
68M10 Network design and communication in computer systems

Keywords:
communication-centred computing; session types; access control; secure information flow

Full Text: DOI

References:
[21] Li, P.; Zdancewic, S., Downgrading policies and relaxed noninterference, (Proc. POPL'05, (2005), ACM Press), 158-170 · Zbl 1369.68146
[23] Pierce, B. C., Types and programming languages, (2002), MIT Press

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.