Disjunctive Information Flow for Communicating Processes

The security validation of practical computer systems calls for the ability to specify and verify information flow policies that are dependent on data content. Such policies play an important role in concurrent, communicating systems: consider a scenario where messages are sent to different processes according to their tagging. We devise a security type system that enforces content-dependent information flow policies in the presence of communication and concurrency. The type system soundly guarantees a compositional noninterference property. All theoretical results have been formally proved in the Coq proof assistant [9].