Symbolic Timed Trace Equivalence

Vivek Nigam, Carolyn Talcott, Abraao Aires Urquiza

Intruders can infer properties of a system by measuring the time it takes for the system to respond to some request of a given protocol, that is, by exploiting time side channels. These properties may help intruders distinguish whether a system is a honeypot or concrete system helping them avoid defense mechanisms, or track a user among others violating his privacy. Observational and trace equivalence are technical machineries used for verifying whether two systems are distinguishable. Automating the check for trace equivalence suffers the state-space explosion problem. Symbolic verification is used to mitigate this problem allowing for the verification of relatively large systems. This paper introduces a novel definition of timed trace equivalence based on symbolic time constraints. Protocol verification problems can then be reduced to problems solvable by off-the-shelf SMT solvers. We implemented such machinery in Maude and carry out a number of experiments demonstrating the feasibility of our approach.