A Calculus for Control Flow Analysis of Security Protocols

The design of a process calculus for analyzing security protocols is governed by three factors: how to express the security protocol in a precise and faithful manner, how to accommodate the variety of attack scenarios, and how to utilize the strengths (and limit the weaknesses) of the underlying analysis methodology. We pursue an analysis methodology based on control flow analysis in flow logic style and we have previously shown its ability to analyze a variety of security protocols. This paper develops a calculus, LysaNS that allows for much greater control and clarity in the description of attack scenarios, that gives a more flexible format for expressing protocols, and that at the same time allows to circumvent some of the "false positives" arising in previous work.