Typing Authentication Protocols in the Presence of Compromised Principals

The use of type systems has proven successful in analyzing security protocols. Some advantages of type-based analyses are that they are efficient and scalable, their termination is guaranteed, and they can be automated. Security requirements and the assumptions made about the capabilities of attackers have significant impact on the design of a type-based analysis method. We present a type-based method to analyze authentication protocols in the presence of compromised principals. It is such that one can verify the highest level of authentication requirements known as injective agreement. The mothod relies on the ideas we have about the modeling of the attackers' capabilities, the specification and verification of authentication requirements, and the security properties that should be reflected by types and typing rules when the environment contains compromised principals. The proposed method is sound and it is provably guaranteed that every well-typed protocol satisfies the specified authentication requirements. We also present a type inference algorithm that automates the analysis in the sense that only a very high-level specification of the protocol and security requirements is required. In order to test the proposed method, we develop a typechekcer implementing the type inference algorithm and analyze various authentication protocols. Experimental results show the efficacy of the proposed method.