A DECIDABLE ANALYSIS OF SECURITY PROTOCOLS

Michael Rusinowitch
LORIA
54602 Villers-lés-Nancy Cedex
France

Cryptographic protocols such as IKE, SET, TLS, Kerberos have been developed to secure electronic transactions. However the design of such protocols often appears to be problematic even assuming that the cryptographic primitives are perfect, i.e. even assuming we cannot decrypt a message without the right key. An intruder may intercept messages, analyse them, modify them with low computing power and then carry out malevolent actions. This may lead to a variety of attacks such as well-known Man-in-the-Middle attacks.

Even in this abstract model, the so-called Dolev-Yao model, protocol analysis is complex since the set of states to consider is huge or infinite. One should consider messages of any size, infinite number of sessions. The interleaving of parallel sessions generates a large search space. Also when we try to relax the perfect encryption hypothesis by taking into account some algebraic properties of operators then the task gets even more difficult.

We will present translation and constraint solving techniques developed in our Cassis team for automating protocol analysis in Dolev-Yao model and some of its extensions. Protocol specifications are compiled and then passed on decision procedures for checking automatically whether they are exposed to flaws.