

Automated verification of security protocols and services

Michaël Rusinowitch ^{*}

LORIA-INRIA-Nancy, France. email: rusi@loria.fr

Abstract. 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 proper key. An intruder may intercept messages, analyse them, modify them without much resources and then carry out malevolent actions. This may lead to a variety of attacks such as well-known Man-In-The-Middle attacks. In this setting, the so-called Dolev-Yao model, protocol analysis can be automated by designing suitable symbolic constraint solving techniques. Messages are represented by terms and intruder actions are simulated by deduction rules. It is also possible to somewhat relax the perfect encryption hypothesis by taking into account some algebraic properties of operators. Secrecy and authentication properties, as expected of correct protocol specifications, are verified by showing that no sequence of intruder actions leads to a failure state.

We present some applications of the same security protocol analysis techniques to service oriented computing such as the synthesis of a secure composed service and its validation. In this original framework intruder actions are replaced by mediator actions and the failure states are replaced by accepting states for both client and services.

^{*} Supported by FP7 Nessos