Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions

Serdar Erbatur[1], Santiago Escobar[2], Deepak Kapur[3], Zhiqiang Liu[4], Christopher Lynch[4], Catherine Meadows[5], José Meseguer[6], Paliath Narendran[1], Sonia Santiago[2], and Ralf Sasse[6]

[1] University at Albany-SUNY, Albany, NY, USA
se@cs.albany.edu, dran@cs.albany.edu
[2] DSIC-ELP, Universitat Politècnica de València, Spain
sescobar@dsic.upv.es,ssantiago@dsic.upv.es
[3] University of New Mexico, Albuquerque, NM, USA
kapur@cs.unm.edu
[4] Clarkson University, Potsdam, NY, USA
liuzh@clarkson.edu, clynch@clarkson.edu
[5] Naval Research Laboratory, Washington DC, USA
meadows@itd.nrl.navy.mil
[6] University of Illinois at Urbana-Champaign, USA
meseguer@illinois.edu, rsasse@illinois.edu

We address a problem that arises in cryptographic protocol analysis when the equational properties of the cryptosystem are taken into account: in many situations it is necessary to guarantee that certain terms generated during a state exploration are in *normal form* with respect to the equational theory. We give a tool-independent methodology for state exploration, based on unification and narrowing, that generates states that obey these irreducibility constraints, called *contextual symbolic reachability analysis*, which we have proven sound and complete, and have implemented in the Maude-NPA protocol analysis tool. Contextual symbolic reachability analysis also introduces a new type of unification mechanism, which we call *asymmetric unification*, in which any solution must leave the right side of the solution irreducible. We also present experiments showing the effectiveness of our methodology.

This 5-minute talk describes a paper that will appear in ESORICS 2012. It will be presented by Catherine Meadows.