The past, present and future of protocol checking with CSP and FDR

Bill Roscoe

The past, present and future of protocol checking with CSP and FDR

Bill Roscoe[1]

Oxford University Computing Laboratory
Oxford, U.K.

Abstract

The prehistory of AVoCS (that is, the series of workshops that gave birth to it) consisted of once or twice annual workshops sponsored by DERA (originally by Peter Ryan) from about 1995, usually held in Oxford or Royal Holloway. The focus of many of these meetings was the development of the CSP model of cryptographic protocols, following Gavin Lowe's discovery that they could be modelled successfully on FDR in 1994. That work led directly or indirectly to most of the formal work done on security protocols since, but naturally many of those whose work was triggered by these discoveries have translated or re-created the ideas in their own notations.

In this talk I will show the particular advantages of using a process algebra, and CSP in particular, for modelling cryptoprotocols, and also some of the problems we have had. I will concentrate on the problem of proving protocols in general, rather than specific small implementations. These methods are based on data independence and in particular the insight of Ranko Lazic that it is possible to get strong results about systems that may include conditional checks for equalities, but not inequalities. In particular, reporting recent joint work with Eldar Kleiner and Tilo Buschmann, I will show how previous work on this topic can be simplified (and automated in Casper) in such a way that it produces remarkably quick proofs or refutations.

This work has led to some interesting insights into the relationship between model checking and other methods of protocol analysis based on strand spaces and Horn clauses.

[1] Email: Bill.Roscoe@comlab.ox.ac.uk

Abstract of an invited talk given at AVoCS 2006
URL: avocs06.loria.fr