Panel: What Protocol Designers Need From Formal Methods

Catherine Meadows
Naval Research Laboratory, Code 5543
Washington, DC 20375
meadows@itd.nrl.navy.mil

The past few years have seen a rapidly growing amount of research in the application of formal methods to the design and verification of cryptographic protocols. They have also seen an equally rapidly growing amount of work in developing and fielding cryptographic protocols, and a growing need for secure communication over the Internet. The problem of assuring the correctness of these protocols has been a matter of some concern, and this sparked interest in making use of the products of formal methods research. However, formal methods has traditionally been seen as an arcane field requiring special expertise, and for this reason difficult to transition into industry.

The purpose of a this panel is to examine the issues around the question of making formal methods for cryptographic protocol analysis into tools that can be used by developers. We have invited a panel of experts on cryptographic protocol development to talk about what they need and expect from formal methods tools and techniques, and in what direction they would like the field to be going. Some of the questions we will be considering are:

1. What problems should formal methods research be addressing that it isn't?
2. Where in the design process do problems most usually appear, and at what level of abstraction? Is it at the level much of the research has been concentrated at, in which messages are modeled as sequences of words encrypted by algorithms that behave as black boxes, is at a lower level involving attacks on algorithms, or is it higher up, at the policy or requirements level? Can this information be used to help formal methods researchers focus their efforts?
3. How could/should formal methods be integrated into the design process? Where can they be of the most help?
4. What are the biggest barriers to using formal methods in cryptographic protocol design?
5. Where are cryptographic protocols going? What are the new applications that will require new types of protocols? In what direction should this be driving research?
6. Are there any new developments in the application of formal methods to cryptographic protocol analysis that seem like they would be particularly useful?
7. Are formal methods researchers making the right assumptions about the mechanisms used by cryptographic protocols and the environments in which they operate? If not, how should they be changed? In particular, do we need a revision of the threat models commonly used?

Panelists

Catherine Meadows, NRL (chair)
John Brainard, RSA
Robert Cordery, Pitney Bowes
Carl Ellison, Cybercash
Steven Kent, BBN