## Preface

Once again we bring you the proceedings of the International Workshop on Security Protocols. It seems hard to believe that we have reached the tenth event in this annual series.

This year our theme was "Discerning the Protocol Participants." Security protocols are usually described in terms of the active participants – Alice computes *foo* and sends it to Bob. However most security protocols also include off-line participants, which are not synchronously involved in the exchange of messages: a bank may participate on behalf of a customer, and an arbiter may subsequently be asked to interpret the meaning of a run.

These silent partners to the protocol have their own security policies, and assumptions about identity, authorization and capability need to be re-examined when the agenda of a hidden participant may change.

We hope that the position papers published here, which have been rewritten and rethought in the light of the discussions at the workshop, will be of interest, not just for the specific contributions they make but also for the deeper issues which they expose. In order to identify these issues more clearly, we include transcripts for some of the discussions which took place in Cambridge during the workshop. What would you have liked to add? Do let us know.

As in past years, these proceedings also include a transcript of the keynote address given by Roger Needham. Alas, this is the last time. Roger's death during the preparation of these proceedings represents a loss, not only to us in the security community but indeed to the whole of computer science, of a magnitude that we are only just beginning to discern. In these proceedings, as in life, he has the last word.

Our thanks to Sidney Sussex College, Cambridge for the use of their facilities, to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes (in which fine grain cement at Wapping nearly proved a sticking point for concurrency) and to Johanna Hunt at the University of Hertfordshire for her assistance in editing the resulting Heraclitian texts.

July 2003

Bruce Christianson
Bruno Crispo
James Malcolm
Michael Roe

**Previous Proceedings in This Series**

The proceedings of previous International Workshops on Security Protocols have also been published by Springer-Verlag as Lecture Notes in Computer Science, and are occasionally referred to in the text:

9th Workshop (2001), LNCS 2467, ISBN 3-540-44263-4
8th Workshop (2000), LNCS 2133, ISBN 3-540-42566-7
7th Workshop (1999), LNCS 1796, ISBN 3-540-67381-4
6th Workshop (1998), LNCS 1550, ISBN 3-540-65663-4
5th Workshop (1997), LNCS 1361, ISBN 3-540-64040-1
4th Workshop (1996), LNCS 1189, ISBN 3-540-63494-5