

Preface

The Cambridge International Workshop on Security Protocols has now run for eight years. Each year we set a theme, focusing upon a specific aspect of security protocols, and invite position papers. Anybody is welcome to send us a position paper (yes, you are invited) and we don't insist they relate to the current theme in an obvious way. In our experience, the emergence of the theme as a unifying thread takes place during the discussions at the workshop itself. The only ground rule is that position papers should formulate an approach to some unresolved issues, rather than being a description of a finished piece of work.

When the participants meet, we try to focus the discussions upon the conceptual issues which emerge. Security protocols link naturally to many other areas of Computer Science, and deep water can be reached very quickly. Afterwards, we invite participants to re-draft their position papers in a way which exposes the emergent issues but leaves open the way to their further development. We also prepare written transcripts of the recorded discussions. These are edited (in some cases very heavily) to illustrate the way in which the different arguments and perspectives have interacted.

We publish these proceedings as an invitation to the research community. Although many interesting results first see the light of day in a volume of our proceedings, laying claim to these is not our primary purpose of publication. Rather, we bring our discussions and insights to a wider audience in order to suggest new lines of investigation which the community may fruitfully pursue.

This year's theme is "Broadening the Protocol Boundary". The boundary of a security protocol has traditionally been drawn very narrowly. Many security protocol "failures" involve factors that were not considered part of the protocol, such as the user interface. In addition, security protocols operate in a naturally fragile environment, and not all threats involve malice on the part of an attacker. Where did Alice get the information she sent, and what is Bob going to do with it? Who and what are the protocol end-points, and which domains are they in?

We invite you to consider these issues with us as you read these proceedings. See you next year, perhaps?

July 2001

Bruce Christianson
Bruno Crispo
James Malcolm
Michael Roe

Acknowledgements

Thanks to Professor Stewart Lee and the University of Cambridge Centre for Communications Systems Research who acted as hosts for the workshop, and to Professor Roger Needham FRS and Microsoft Research Limited (Cambridge) who provided us with the use of their meeting room and coffee machine. Plaudits of gratitude also to Dorian Addison of CCSR and to Angela Leeke and Margaret Nicell of MSRL for impeccable organization and administration, to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes (including the static which changed a word attachment into a work of passion) and to Dr Mary Buchannan for her Procrustean editorial assistance.

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:

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

Security Protocols

8th International Workshops Cambridge, UK, April 3-5,

2000 Revised Papers

Christianson, B.; Crispo, B.; Malcolm, J.A.; Roe, M. (Eds.)

2001, VIII, 264 p., Softcover

ISBN: 978-3-540-42566-3