Preface

You hold in your hands the proceedings of the sixth Cambridge International Workshop on Security Protocols. This annual event is an opportunity for researchers in acadaemia and industry to discuss new developments in the area of distributed system security, using various insights into the general notion of a protocol as a point of departure. Although you will also find plenty of interesting new results in this volume, our primary concern is to create a forum in which researchers are free to discuss the limitations of current work: things we can't yet do, or don't yet fully understand.

This year the theme of the workshop was the interactions between trust and delegation, exploring the implications and effects of these upon such issues as authorization, security policy and system and component design. As you will see, this turned out to be a fruitful avenue. This volume marks a return to our original intention for the format of the proceedings: we bring you a short position paper from each contributor, deliberately written to provoke reasoned controversy, together with not-quite-verbatim transcripts of the discussions which ensued.

Many thanks to Stewart Lee and the University of Cambridge Centre for Communications Systems Research, for acting as hosts of the workshop, and to Roger Needham and Microsoft Research Limited (Cambridge), for providing us with an excellent venue and large amounts of coffee. This year's workshop marks twenty years since the publication of Needham and Schroeder's "Using Encryption for Authentication in Large Networks of Computers" and ten years since the first appearance of the BAN logic, so we were delighted to have Roger in the chair for the final panel discussion, a transcript of which concludes the volume.

It is a pleasure to express our gratitude to Hitachi and Nortel for providing financial support. We are also indebted to Robin Milner of the University of Cambridge Computer Laboratory for his support and assistance. Finally, we would like to thank Dorian Addison of CCSR for undertaking a Sisyphean burden of administration, and Lori Klimaszewska of the University of Cambridge Computing Service for an excellent job of transcribing audio tapes full of "techie-talk and coughing".

We use this workshop to guide our own research agendas, and we hope that engaging with the discussions in these proceedings will also provide you with some useful reflections upon your research, and maybe help inspire it in some unexpected new direction. If this happens please write and tell us, we'd love to hear from you.

Bruce Christianson
Bruno Crispo
William Harbison
Michael Roe

http://www.springer.com/978-3-540-65663-0

Security Protocols
6th International Workshop, Cambridge, UK, April 15-17, 1998, Proceedings
Christianson, B.; Crispo, B.; Harbison, W.S.; Roe, M. (Eds.)
1999, VIII, 252 p., Softcover
ISBN: 978-3-540-65663-0