Bruce Christianson  Bruno Crispo
William S. Harbison  Michael Roe (Eds.)

Security Protocols

6th International Workshop
Cambridge, UK, April 15-17, 1998
Proceedings

Springer
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 academia 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 Klimaszewksa 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
Contents

Inductive Analysis of the Internet Protocol TLS
  Lawrence C. Paulson ......................................... 1
  Discussion .................................................. 13

External Consistency and the Verification of Security Protocols
  Simon N. Foley ............................................... 24
  Discussion .................................................. 28

The Trust Shell Game
  Carl Ellison .................................................. 36
  Discussion .................................................. 41

Overview of the AT&T Labs Trust-Management Project
  Joan Feigenbaum ............................................. 45
  Discussion .................................................. 51

KeyNote: Trust Management for Public-Key Infrastructures
  Matt Blaze, Joan Feigenbaum, Angelos D. Keromytis* .............. 59
  Discussion .................................................. 64

Application-Oriented Security Policies and Their Composition
  Virgil D. Gligor* and Serban I. Gavrila .......................... 67
  Discussion .................................................. 75

Secure Fingerprinting Using Public-Key Cryptography
  Hiroshi Yoshiura, Ryoichi Sasaki* and Kazuo Takaragi ............ 83
  Discussion .................................................. 90

Third Party Certification of HTTP Service Access Statistics
  Francesco Bergadano* and Pancrazi De Mauro ...................... 95
  Discussion .................................................. 100

Delegating Trust
  William S. Harbison (Discussion) ................................ 108

Delegation of Responsibility
  Bruno Crispo ................................................ 118
  Discussion .................................................. 125

Abuse of Process
  Mark Lomas (Discussion) .................................... 131
A New Concept in Protocols: Verifiable Computational Delegation

Peter Landrock ................................................................. 137
Discussion ................................................................. 146

Delegation and Not-So Smart Cards

Bruce Christianson* and James A. Malcolm ............................. 154
Discussion ................................................................. 158

Certification and Delegation

Michael Roe (Discussion) ...................................................... 168

Discussion - Differences Between Academic and Commercial Security

Virgil Gligor, Peter Landrock, Mark Lomas, Raphael Yahalom
and John Warne ................................................................. 177

Optimistic Trust with Realistic eNvestigators

Raphael Yahalom ................................................................. 193
Discussion ................................................................. 203

Insider Fraud

Dieter Gollmann ................................................................. 213
Discussion ................................................................. 220

Panel Session - Future Directions

Stewart Lee, Joan Feigenbaum, Virgil Gligor and Bruce Christianson
Chair: Roger Needham ................................................................. 227

Contributor Index ................................................................. 241