Lecture Notes in Computer Science 2467

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Bruce Christianson Bruno Crispo
James A. Malcolm Michael Roe (Eds.)

Security Protocols

9th International Workshop
Cambridge, UK, April 25-27, 2001
Revised Papers

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Bruce Christianson
James A. Malcolm
University of Hertfordshire, Department of Computer Science
Faculty of Engineering and Information Sciences
College Lane, Hatfield, Herts, AL10 9AB, UK
E-mail: {b.christianson/J.A.Malcolm}@herts.ac.uk

Bruno Crispo
Vrije Universiteit, Department of Computer Science
De Boelelaan 1081A, 1081 HV Amsterdam, The Netherlands
E-mail: crispo@cs.vu.nl

Michael Roe
Microsoft Research Limited
7 J J Thomson Avenue, Cambridge, CB3 0FB, UK
E-mail: mroe@microsoft.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Security protocols : 9th international workshop, Cambridge, UK, April 25 - 27, 2001 ; revised papers / Bruce Christianson ... (ed.). - Berlin ; Heidelberg ; New York ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2467)
ISBN 3-540-44263-4

CR Subject Classification (1998): E.3, F.2.1-2, C.2, K.6.5, J.1, K.4.1, D.4.6

ISSN 0302-9743
ISBN 3-540-44263-4 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN 10871275 06/3142 5 4 3 2 1 0

Preface

Hello and welcome. These are the proceedings of the 9th International Workshop on Security Protocols, the first to be held in the new millennium. This year our theme was "mobile computing versus immobile security". As usual, the insights and challenges which emerged during the workshop are reflected in the position papers, which appear here in rewritten form.

Transcripts are also included of the discussions which took place in Cambridge as the initial versions were presented. These transcripts are intended to provide a perspective on lines of argument which are worth pursuing further. Our desire is that you will join with us in this activity, and that as a result you will, like many of our participants, feel moved to propound something quite different from what you originally planned.

Our thanks as always to Prof. Roger Needham, FRS and to Microsoft Research Ltd. (Cambridge) for the use of the meeting room and coffee machine. Thanks also to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes (and for revealing in "Audrey James" a previously unsuspected double life of a well-known double agent), and to Dr. Mary Buchanan for her assistance in editing the transcripts into a Thucydidean mould.

Actually, we are often asked how we go about producing the transcripts, especially upon those occasions when, for various reasons, no audio recording was made. This year we bow to pressure and reveal the details of our methodology in the Afterword.

We hope you find these proceedings enjoyable, infuriating, and fruitful. And we look forward to hearing from you.

Christmas Eve 2001

Bruce Christianson
Bruno Crispo
James Malcolm
Michael Roe

Previous Proceedings in This Series

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

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

Table of Contents