

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

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 Klimaszevska 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

Keynote Address: Mobile Computing versus Immobile Security	1
<i>Roger Needham</i>	
Experiences of Mobile IP Security (Transcript of Discussion)	4
<i>Michael Roe</i>	
Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World	12
<i>Pekka Nikander</i>	
Denial of Service, Address Ownership, and Early Authentication in the IPv6 World (Transcript of Discussion)	22
<i>Pekka Nikander</i>	
Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols	27
<i>William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold</i>	
Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols (Transcript of Discussion)	40
<i>Matt Blaze</i>	
Thwarting Timing Attacks Using ATM Networks	49
<i>Geraint Price</i>	
Thwarting Timing Attacks Using ATM Networks (Transcript of Discussion)	59
<i>Geraint Price</i>	
Towards a Survivable Security Architecture for Ad-Hoc Networks	63
<i>Tuomas Aura, Silja Mäki</i>	
Towards a Survivable Security Architecture for Ad-Hoc Networks (Transcript of Discussion)	74
<i>Silja Mäki</i>	
PIM Security	80
<i>Dieter Gollmann</i>	
PIM Security (Transcript of Discussion)	82
<i>Dieter Gollmann</i>	
Merkle Puzzles Revisited – Finding Matching Elements between Lists	87
<i>Bruce Christianson, David Wheeler</i>	

Merkle Puzzles Revisited (Transcript of Discussion) 91
Bruce Christianson

Encapsulating Rules of Prudent Security Engineering (Position Paper).... 95
Jan Jürjens

Encapsulating Rules of Prudent Security Engineering
(Transcript of Discussion) 102
Jan Jürjens

A Multi-OS Approach to Trusted Computer Systems 107
*Hiroshi Yoshiura, Kunihiko Miyazaki, Shinji Itoh, Kazuo Takaragi,
Ryoichi Sasaki*

A Multi-OS Approach to Trusted Computer Systems (Transcript
of Discussion) 115
Hiroshi Yoshiura

A Proof of Non-repudiation 119
Giampaolo Bella, Lawrence C. Paulson

A Proof of Non-repudiation (Transcript of Discussion) 126
Larry Paulson

Using Authority Certificates to Create
Management Structures..... 134
Babak Sadighi Firozabadi, Marek Sergot, Olav Bandmann

Using Attribute Certificates for Creating Management
Structures (Transcript of Discussion) 146
Babak Sadighi Firozabadi

Trust Management and Whether to Delegate 151
Simon N. Foley

Trust Management and Whether to Delegate (Transcript
of Discussion) 158
Simon N. Foley

You Can't Take It with You (Transcript of Discussion) 166
Mark Lomas

Protocols Using Keys from Faulty Data 170
David Wheeler

Protocols Using Keys from Faulty Data (Transcript of Discussion) 180
David Wheeler

On the Negotiation of Access Control Policies	188
<i>Virgil D. Gligor, Himanshu Khurana, Radostina K. Koleva,</i> <i>Vijay G. Bharadwaj, John S. Baras</i>	
Negotiation of Access Control Policies (Transcript of Discussion)	202
<i>Virgil D. Gligor</i>	
Intrusion-Tolerant Group Management in Enclaves (Transcript of Discussion)	213
<i>Hassen Saïdi</i>	
Lightweight Authentication in a Mobile Network (Transcript of Discussion)	217
<i>James Malcolm</i>	
Bluetooth Security — Fact or Fiction? (Transcript of Discussion)	221
<i>Peter Drabwell</i>	
Concluding Discussion When Does Confidentiality Harm Security?	229
<i>Chair: Bruce Christianson</i>	
The Last Word	239
<i>Thucydides</i>	
Author Index	241