Lecture Notes in Computer Science 3364

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Security Protocols

11th International Workshop
Cambridge, UK, April 2-4, 2003
Revised Selected Papers

Springer

Volume Editors

Bruce Christianson
James A. Malcolm
University of Hertfordshire
Computer Science Department
Hatfield AL10 9AB, UK
E-mail: {b.christianson,J.A.Malcolm}@herts.ac.uk

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

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

Library of Congress Control Number: 2005931713

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-10 3-540-28389-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28389-8 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11542322 06/3142 5 4 3 2 1 0

Preface

Greetings. These are the proceedings of the 11th in our series of International Workshops on Security Protocols. Our theme this time was “Where have all the Protocols gone?” Once upon a time security protocols lived mainly in the network and transport layers. Now they increasingly hide in applications, or in specialised hardware. Does this trend lead to better security architectures, or is it an indication that we are addressing the wrong problems?

The intention of the workshops is to provide a forum where incompletely worked out ideas can stimulate discussion, open up new lines of investigation, and suggest more problems. The position papers published here have been revised by the authors in the light of their participation in the workshop. In addition, we publish edited transcripts of some of the discussions, to give our readers access to some of the roads ahead not (yet) taken. We hope that these revised position papers and edited transcripts will give you at least one interesting idea of your own to explore. Please do write and tell us what it was.

Our purpose in publishing these proceedings is to produce a conceptual map which will be of enduring interest, rather than to be merely topical. This is perhaps just as well, given the delay in production. This year we moved to new computer-based recording technology, and of course it failed completely. Fortunately various domestic recorders had been smuggled into the venue, but picking the signal bits out of the noise has taken a long time, and we have had to insert more than the usual number of epicycles to make the discussions come out right.

Our thanks to Sidney Sussex College Cambridge for the use of their facilities, to Lori Klimaszewska of the University of Cambridge Computing Service for the even worse than usual task of transcribing the audio tapes (in which the reverse use of “two rings” provided a test for creative intelligence) and to Johanna Hunt at the University of Hertfordshire for helping us with the Ptolemeic editing of the results.

Lent 2005

Bruce Christianson
Bruno Crispo
James Malcolm
Michael Roe

Previous Proceedings in This Series

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

10th Workshop (2002), LNCS 2845, ISBN 3-540-20830-5
9th Workshop (2001), LNCS 2467, ISBN 3-540-44263-4
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

Where Have All the Protocols Gone?
Bruce Christianson 1

A Protocol's Life After Attacks...
*Giampaolo Bella**, *Stefano Bistarelli, Fabio Massacci* 3
Discussion 11

Towards Flexible Credential Negotiation Protocols
Piero A. Bonatti, Sabrina De Capitani di Vimercati,
*Pierangela Samarati** 19
Discussion 24

Man-in-the-Middle in Tunnelled Authentication Protocols
*N. Asokan**, *Valtteri Niemi, Kaisa Nyberg* 28
Discussion 42

Towards a Framework for Autonomic Security Protocols
*Simon N. Foley**, *Hongbin Zhou* 49
Discussion 55

Client v. Server Side Protocols, Interfaces and Storage
Geraint Price 63
Discussion 74

Guaranteeing Access in Spite of Distributed Service-Flooding Attacks
Virgil D. Gligor 80
Discussion 97

Protocol Codesign
*Hassen Saïdi, Victoria Stavridou**, *Bruno Duterte* 106
Discussion 114

Enforcing Security Policies for Distributed Objects Applications
*Bogdan C. Popescu**, *Bruno Crispo, Andrew S. Tanenbaum,*
Maas Zeeman 119
Discussion 131

* Speakers.

Regular SPKI
Mads Dam 134
Discussion 151

Federated Identity-Management Protocols
*Birgit Pfitzmann**, *Michael Waidner* 153
Discussion 175

Enforcing the Unenforceable
Peter Y.A. Ryan 178

Is the Verification Problem for Cryptographic Protocols Solved?
*Giampaolo Bella, Cristiano Longo, Lawrence Paulson** 183

Secure Sessions from Weak Secrets
*Bruce Christianson**, *Michael Roe, David Wheeler* 190
Discussion 206

Panel Session: Is Protocol Modelling Finished?
Mike Roe 213

WAR: Wireless Anonymous Routing
*Matt Blaze**, *John Ioannidis, Angelos D. Keromytis, Tal Malkin,*
Avi Rubin 218
Discussion 233

Limitations of IPsec Policy Mechanisms
*Jari Arkko**, *Pekka Nikander* 241
Discussion 252

Deniable Authenticated Key Establishment for Internet Protocols
*Colin Boyd, Wenbo Mao**, *Kenneth G. Paterson* 255
Discussion 272

Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks
*Mike Burmester, Alec Yasinsac** 274
Discussion 283

What We Can Learn from API Security
Ross Anderson 288

Addressing New Challenges by Building Security Protocols Around Graphs
*Kamil Kulesza**, *Zbigniew Kotulski* 301

From Security Protocols to System Security
Brian Monahan 307
Discussion 323

Biometrics to Enhance Smartcard Security
*Giampaolo Bella, Stefano Bistarelli, Fabio Martinelli** 324
Discussion 333

Blind Publication: A Copyright Library without Publication or Trust
James A. Malcolm 336
Discussion 341

And Finally 350

Author Index 351