Lecture Notes in Computer Science 5087

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

14th International Workshop
Cambridge, UK, March 27-29, 2006
Revised Selected Papers

Springer

Volume Editors

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

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

James A. Malcolm
University of Hertfordshire, Computer Science Department
Hatfield, AL10 9AB, UK
E-mail: j.a.malcolm@herts.ac.uk

Michael Roe
Microsoft Research Ltd., Roger Needham Building
7 JJ Thomson Avenue, Cambridge, CB3 0FB, UK
E-mail: mroe@microsoft.com

Library of Congress Control Number: 2009935708

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, K.4, F.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-04903-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04903-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12771844 06/3180 5 4 3 2 1 0

Preface

Welcome back to the International Security Protocols Workshop. Our theme for this, the 14th workshop in the series, is "Putting the Human Back in the Protocol".

We've got into the habit of saying "Of course, Alice and Bob aren't really people. Alice and Bob are actually programs running in some computers." But we build computer systems in order to enable people to interact in accordance with certain social protocols. So if we're serious about system services being end-to-end then, at some level of abstraction, the end points Alice and Bob are human after all. This has certain consequences. We explore some of them in these proceedings, in the hope that this will encourage you to pursue them further. Is Alice talking to the correct stranger?

Our thanks to Sidney Sussex College, Cambridge for the use of their facilities, and to the University of Hertfordshire for lending us several of their staff. Particular thanks once again to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes, and to Virgil Gligor for acting as our advisor.

August 2009

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:

13th Workshop (2005), LNCS 4631, ISBN 3-540-77155-7
12th Workshop (2004), LNCS 3957, ISBN 3-540-40925-4
11th Workshop (2003), LNCS 3364, ISBN 3-540-28389-7
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

Putting the Human Back in the Protocol (Transcript of Discussion) 1
Bruce Christianson

Composing Security Metrics (Transcript of Discussion) 3
Matt Blaze

Putting the Human Back in Voting Protocols 13
Peter Y.A. Ryan and Thea Peacock

Putting the Human Back in Voting Protocols (Transcript of Discussion) 20
Peter Y.A. Ryan

Towards a Secure Application-Semantic Aware Policy Enforcement Architecture 26
Srijith K. Nair, Bruno Crispo, and Andrew S. Tanenbaum

Towards a Secure Application-Semantic Aware Policy Enforcement Architecture (Transcript of Discussion) 32
Srijith K. Nair

Phish and Chips: Traditional and New Recipes for Attacking EMV 40
Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, Ross Anderson, and Ron Rivest

Phish and Chips (Transcript of Discussion) 49
Mike Bond

Where Next for Formal Methods? 52
James Heather and Kun Wei

Where Next for Formal Methods? (Transcript of Discussion) 59
James Heather

Cordial Security Protocol Programming: The Obol Protocol Language 62
Per Harald Myrvang and Tage Stabell-Kulø

Cordial Security Protocol Programming (Transcript of Discussion) 85
Tage Stabell-Kulø

Privacy-Sensitive Congestion Charging 97
Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle

Privacy-Sensitive Congestion Charging (Transcript of Discussion) 105
Alastair R. Beresford

The Value of Location Information: A European-Wide Study 112
Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis

The Value of Location Information (Transcript of Discussion)..... 122
Vashek Matyas

Update on PIN or Signature (Transcript of Discussion) 128
Vashek Matyas

Innovations for Grid Security from Trusted Computing: Protocol Solutions to Sharing of Security Resource 132
Wenbo Mao, Andrew Martin, Hai Jin, and Huanguo Zhang

Innovations for Grid Security from Trusted Computing (Transcript of Discussion)..... 150
Wenbo Mao

The Man-in-the-Middle Defence 153
Ross Anderson and Mike Bond

The Man-in-the-Middle Defence (Transcript of Discussion) 157
Ross Anderson

Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries 164
Chris J. Mitchell

Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries (Transcript of Discussion) 171
Chris J. Mitchell

Secure Distributed Human Computation (Extended Abstract) 177
Craig Gentry, Zulfikar Ramzan, and Stuart Stubblebine

Secure Distributed Human Computation (Transcript of Discussion)..... 181
Craig Gentry

Bot, Cyborg and Automated Turing Test (Or "Putting the Humanoid in the Protocol")..... 190
Jeff Yan

Bot, Cyborg and Automated Turing Test (Transcript of Discussion) 198
Jeff Yan

A 2-Round Anonymous Veto Protocol 202
Feng Hao and Piotr Zieliński

A 2-Round Anonymous Veto Protocol (Transcript of Discussion) 212
Feng Hao

How to Speak an Authentication Secret Securely from an Eavesdropper 215
Lawrence O'Gorman, Lynne Brotman, and Michael Sammon

How to Speak an Authentication Secret Securely from an Eavesdropper (Transcript of Discussion) 230
Lawrence O'Gorman

Secret Public Key Protocols Revisited 237
Hoon Wei Lim and Kenneth G. Paterson

Secret Public Key Protocols Revisited (Transcript of Discussion) 257
Hoon Wei Lim

Vintage Bit Cryptography 261
Bruce Christianson and Alex Shafarenko

Vintage Bit Cryptography (Transcript of Discussion) 266
Alex Shafarenko

Usability of Security Management: Defining the Permissions of Guests 276
Matthew Johnson and Frank Stajano

Usability of Security Management: Defining the Permissions of Guests (Transcript of Discussion) 284
Matthew Johnson

The Last Word 286
Eve

Author Index 287