

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

Security Protocols

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

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

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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

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) <i>Bruce Christianson</i>	1
Composing Security Metrics (Transcript of Discussion) <i>Matt Blaze</i>	3
Putting the Human Back in Voting Protocols <i>Peter Y.A. Ryan and Thea Peacock</i>	13
Putting the Human Back in Voting Protocols (Transcript of Discussion) <i>Peter Y.A. Ryan</i>	20
Towards a Secure Application-Semantic Aware Policy Enforcement Architecture <i>Srijith K. Nair, Bruno Crispo, and Andrew S. Tanenbaum</i>	26
Towards a Secure Application-Semantic Aware Policy Enforcement Architecture (Transcript of Discussion) <i>Srijith K. Nair</i>	32
Phish and Chips: Traditional and New Recipes for Attacking EMV <i>Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, Ross Anderson, and Ron Rivest</i>	40
Phish and Chips (Transcript of Discussion) <i>Mike Bond</i>	49
Where Next for Formal Methods? <i>James Heather and Kun Wei</i>	52
Where Next for Formal Methods? (Transcript of Discussion) <i>James Heather</i>	59
Cordial Security Protocol Programming: The Obol Protocol Language <i>Per Harald Myrvang and Torgeir Stabell-Kulø</i>	62
Cordial Security Protocol Programming (Transcript of Discussion) <i>Torgeir Stabell-Kulø</i>	85
Privacy-Sensitive Congestion Charging <i>Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle</i>	97

Privacy-Sensitive Congestion Charging (Transcript of Discussion)	105
<i>Alastair R. Beresford</i>	
The Value of Location Information: A European-Wide Study	112
<i>Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis</i>	
The Value of Location Information (Transcript of Discussion)	122
<i>Vashek Matyas</i>	
Update on PIN or Signature (Transcript of Discussion)	128
<i>Vashek Matyas</i>	
Innovations for Grid Security from Trusted Computing: Protocol Solutions to Sharing of Security Resource	132
<i>Wenbo Mao, Andrew Martin, Hai Jin, and Huanguo Zhang</i>	
Innovations for Grid Security from Trusted Computing (Transcript of Discussion)	150
<i>Wenbo Mao</i>	
The Man-in-the-Middle Defence	153
<i>Ross Anderson and Mike Bond</i>	
The Man-in-the-Middle Defence (Transcript of Discussion)	157
<i>Ross Anderson</i>	
Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries	164
<i>Chris J. Mitchell</i>	
Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries (Transcript of Discussion)	171
<i>Chris J. Mitchell</i>	
Secure Distributed Human Computation (Extended Abstract)	177
<i>Craig Gentry, Zulfikar Ramzan, and Stuart Stubblebine</i>	
Secure Distributed Human Computation (Transcript of Discussion)	181
<i>Craig Gentry</i>	
Bot, Cyborg and Automated Turing Test (Or “Putting the Humanoid in the Protocol”)	190
<i>Jeff Yan</i>	
Bot, Cyborg and Automated Turing Test (Transcript of Discussion)	198
<i>Jeff Yan</i>	
A 2-Round Anonymous Veto Protocol	202
<i>Feng Hao and Piotr Zielinski</i>	

A 2-Round Anonymous Veto Protocol (Transcript of Discussion)	212
<i>Feng Hao</i>	
How to Speak an Authentication Secret Securely from an Eavesdropper	215
<i>Lawrence O’Gorman, Lynne Brotman, and Michael Sammon</i>	
How to Speak an Authentication Secret Securely from an Eavesdropper (Transcript of Discussion)	230
<i>Lawrence O’Gorman</i>	
Secret Public Key Protocols Revisited	237
<i>Hoon Wei Lim and Kenneth G. Paterson</i>	
Secret Public Key Protocols Revisited (Transcript of Discussion)	257
<i>Hoon Wei Lim</i>	
Vintage Bit Cryptography	261
<i>Bruce Christianson and Alex Shafarenko</i>	
Vintage Bit Cryptography (Transcript of Discussion)	266
<i>Alex Shafarenko</i>	
Usability of Security Management: Defining the Permissions of Guests	276
<i>Matthew Johnson and Frank Stajano</i>	
Usability of Security Management: Defining the Permissions of Guests (Transcript of Discussion)	284
<i>Matthew Johnson</i>	
The Last Word	286
<i>Eve</i>	
Author Index	287