

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

TU Dortmund University, 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 for Informatics, Saarbruecken, Germany

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

Security Protocols

15th International Workshop
Brno, Czech Republic, April 18-20, 2007
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
Dipartimento di Ingegneria e Scienza dell'Informazione
Via Sommarive 14, 38123 Povo (TN), Italy
E-mail: bruno.crispo@unitn.it

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@cornstalk.org.uk

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-17772-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-17772-9 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 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

Welcome once again to the proceedings of the International Security Protocols Workshop. The 15th workshop in our series took place in Brno, a beautiful city in the southeast of the Czech Republic famous also as setting for a blown espionage operation in “Tinker Tailor Soldier Spy.”

The theme of our deliberations this time was: “When is a Protocol Broken?”. We expect network protocols to degrade gracefully when their assumptions are broken, and even to recover from the error. Network protocol designers spend as much time thinking about recovery as about preventing failures in the first place, but we do not tend to think about recovering from a security protocol failure at all. Loss of confidentiality seems hard to reverse, but integrity and authentication are far more important security requirements in practice. How can (or should) we make security protocols more flexible at adapting to changed assumptions?

Our thanks are due to Vashek Matyas, Marek Kumpost and their colleagues from Masaryk University for the considerable work of organizing the event. Particular thanks once again to Lori Klimaszevska of the University of Cambridge Computing Service for transcribing the audio tapes, and to Vashek Matyas and Virgil Gligor for acting as members of the Programme Committee.

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:

14th Workshop (2006), LNCS 5087, ISBN 978-3-642-04903-3
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

When Is a Protocol Broken? (Transcript of Discussion)	1
<i>Bruce Christianson</i>	
Measurable Security through Isotropic Channels	3
<i>Micah Sherr, Eric Cronin, and Matt Blaze</i>	
Measurable Security through Isotropic Channels (Transcript of Discussion)	13
<i>Micah Sherr</i>	
Modeling Partial Attacks with ALLOY	20
<i>Amerson Lin, Mike Bond, and Jolyon Clulow</i>	
Modeling Partial Attacks with ALLOY (Transcript of Discussion)	34
<i>Amerson Lin</i>	
Resiliency Aspects of Security Protocols	37
<i>Marcus C. Granado</i>	
Privacy Amplification with Social Networks	58
<i>Shishir Nagaraja</i>	
Privacy Amplification with Social Networks (Transcript of Discussion)	74
<i>Shishir Nagaraja</i>	
Reconciling Multiple IPsec and Firewall Policies	81
<i>Tuomas Aura, Moritz Becker, Michael Roe, and Piotr Zielinski</i>	
Reconciling Multiple IPsec and Firewall Policies (Transcript of Discussion)	98
<i>Michael Roe</i>	
Anchor-Less Secure Session Mobility	104
<i>Alf Zugenmaier, Julien Laganier, Anand Prasad, and Kristian Slavov</i>	
Anchor-Less Secure Session Mobility (Transcript of Discussion)	110
<i>Alf Zugenmaier</i>	
A Model for System-Based Analysis of Voting Systems	114
<i>Thomas Tjøstheim, Thea Peacock, and Peter Y.A. Ryan</i>	
A Model for System-Based Analysis of Voting Systems (Transcript of Discussion)	131
<i>Thomas Tjøstheim</i>	

Multi-Channel Key Agreement Using Encrypted Public Key Exchange	133
<i>Bruce Christianson and Jun Li</i>	
Multi-Channel Key Agreement Using Encrypted Public Key Exchange (Transcript of Discussion)	139
<i>Bruce Christianson</i>	
On the Security of the EMV Secure Messaging API (Extended Abstract)	147
<i>Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ross Anderson, and Ronald L. Rivest</i>	
On the Security of the EMV Secure Messaging API (Transcript of Discussion)	150
<i>Jolyon Clulow</i>	
Distributed Double Spending Prevention	152
<i>Jaap-Henk Hoepman</i>	
Distributed Double Spending Prevention (Transcript of Discussion)	166
<i>Jaap-Henk Hoepman</i>	
Robbing the Bank with a Theorem Prover (Abstract)	171
<i>Paul YOUN, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ronald L. Rivest, and Ross Anderson</i>	
Robbing the Bank with a Theorem Prover (Transcript of Discussion) . . .	172
<i>Jolyon Clulow</i>	
Disclosure Control of Natural Language Information to Enable Secure and Enjoyable Communication over the Internet	178
<i>Haruno Kataoka, Akira Utsumi, Yuki Hirose, and Hiroshi Yoshiura</i>	
Disclosure Control of Natural Language Information to Enable Secure and Enjoyable Communication over the Internet (Transcript of Discussion)	189
<i>Hiroshi Yoshiura</i>	
Towards Working with Small Atomic Functions	191
<i>Alec Yasinsac and J. Todd McDonald</i>	
Towards Working with Small Atomic Functions (Transcript of Discussion)	201
<i>Alec Yasinsac</i>	
Daonity: Protocol Solutions to Grid Security Using Hardware Strengthened Software Environment	204
<i>Wenbo Mao, Fei Yan, Chuanjiang Yi, and Haibo Chen</i>	

Private Yet Abuse Resistant Open Publishing	222
<i>George Danezis and Ben Laurie</i>	
Private Yet Abuse Resistant Open Publishing (Transcript of Discussion)	244
<i>George Danezis</i>	
Instructions to Reviewers	256
Author Index	257