

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 James Malcolm
Frank Stajano Jonathan Anderson (Eds.)

Security Protocols XX

20th International Workshop
Cambridge, UK, April 12-13, 2012
Revised Selected Papers

 Springer

Volume Editors

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

Frank Stajano
Jonathan Anderson
University of Cambridge
Computer Laboratory
15 JJ Thomson Avenue, Cambridge, CB3 0FD, UK
E-mail: {frank.stajano, jonathan.anderson}@cl.cam.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-35693-3 e-ISBN 978-3-642-35694-0
DOI 10.1007/978-3-642-35694-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012954009

CR Subject Classification (1998): C.2, K.6.5, E.3, D.4.6, H.3-4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume collects the revised proceedings of the 20th International Security Protocols Workshop, held in Sidney Sussex College, Cambridge, during April 12–13, 2012. The theme of the workshop was “Bringing Protocols to Life.” We are getting steadily better at specifying security protocols, but can we reason about their subtle interactions with the real world: with the environment, the application, and the system resources?

As with previous workshops in this series, each paper was revised by the authors to incorporate ideas that emerged during the workshop. These revised papers are followed by an edited transcript of the presentation and ensuing discussion. As happened last year, thanks to the valiant effort of all the workshop participants, this proceedings volume is published in the same year as the workshop.

Our thanks to Lori Klimaszezewska for the raw transcriptions of the audio, later revised by the speakers themselves, and to Vashek Matyas and Michael Roe for serving with us on the Program Committee. Thanks also to Microsoft Research for financial support.

This workshop being the 20th, we introduced the Roger Needham Award for the paper that provoked the most interesting discussion. Each speaker ranked the papers, and following a Single Transferable Vote protocol the award was won by Sandy Clark, Matt Blaze and Jonathan Smith, for their paper on “The Casino and the OODA Loop.”

Participation in the Security Protocols Workshop is by personal invitation following submission of a position paper. If you would like your position paper to be considered for the next workshop, please get in touch.

As always, our hope in disseminating these papers, and the debates that they engendered, is to encourage you to engage with these issues yourselves.

September 2012

Bruce Christianson
James Malcolm
Frank Stajano
Jonathan Anderson

Previous Proceedings in This Series

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

19th Workshop (2011)	LNCS 7114	ISBN 978-3-642-25866-4
18th Workshop (2010)	LNCS 7061	<i>in preparation</i>
17th Workshop (2009)	LNCS 7028	<i>in press</i>
16th Workshop (2008)	LNCS 6615	ISBN 978-3-642-22136-1
15th Workshop (2007)	LNCS 5964	ISBN 978-3-642-17772-9
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

No published proceedings exist for the first three workshops.

Table of Contents

Introduction: Bringing Protocols to Life (Transcript of Discussion)	1
<i>Bruce Christianson</i>	
Secure Internet Voting Protocol for Overseas Military Voters	3
<i>Todd R. Andel and Alec Yasinsac</i>	
Secure Internet Voting Protocol for Overseas Military Voters (Transcript of Discussion)	15
<i>Todd R. Andel</i>	
Self-enforcing Electronic Voting	23
<i>Feng Hao, Brian Randell, and Dylan Clarke</i>	
Self-enforcing Electronic Voting (Transcript of Discussion)	32
<i>Feng Hao</i>	
Approaches to Modelling Security Scenarios with Domain-Specific Languages	41
<i>Phillip J. Brooke, Richard F. Paige, and Christopher Power</i>	
Approaches to Modelling Security Scenarios with Domain-Specific Languages (Transcript of Discussion)	55
<i>Phillip J. Brooke</i>	
The Casino and the OODA Loop: Why Our Protocols Always Eventually Fail	60
<i>Sandy Clark, Matt Blaze, and Jonathan M. Smith</i>	
The Casino and the OODA Loop: Why Our Protocols Always Eventually Fail (Transcript of Discussion)	64
<i>Matt Blaze</i>	
Statistical Metrics for Individual Password Strength	76
<i>Joseph Bonneau</i>	
Statistical Metrics for Individual Password Strength (Transcript of Discussion)	87
<i>Joseph Bonneau</i>	
Street-Level Trust Semantics for Attribute Authentication	96
<i>Tiffany Hyun-Jin Kim, Virgil Gligor, and Adrian Perrig</i>	
Street-Level Trust Semantics for Attribute Authentication (Transcript of Discussion)	116
<i>Virgil Gligor</i>	

Analysis of Issues and Challenges of E-Voting in the UK	126
<i>Dylan Clarke, Feng Hao, and Brian Randell</i>	
Analysis of Issues and Challenges of E-Voting in the UK (Transcript of Discussion)	136
<i>Dylan Clarke</i>	
Protocol Governance: The Elite, or the Mob?	145
<i>Ross Anderson</i>	
Protocol Governance: The Elite, or the Mob? (Transcript of Discussion)	146
<i>Ross Anderson</i>	
Usability Issues in Security	161
<i>Yuko Murayama, Yasuhiro Fujihara, Yoshia Saito, and Dai Nishioka</i>	
Usability Issues in Security (Transcript of Discussion)	172
<i>Yuko Murayama</i>	
Usable Privacy by Visual and Interactive Control of Information Flow	181
<i>Shah Mahmood and Yvo Desmedt</i>	
Usable Privacy by Visual and Interactive Control of Information Flow (Transcript of Discussion)	189
<i>Shah Mahmood</i>	
Sense-And-Trace: A Privacy Preserving Distributed Geolocation Tracking System	199
<i>Eyüp S. Canlar, Mauro Conti, Bruno Crispo, and Roberto Di Pietro</i>	
Sense-And-Trace: A Privacy Preserving Distributed Geolocation Tracking System (Transcript of Discussion)	214
<i>Mauro Conti</i>	
Am I in Good Company? A Privacy-Protecting Protocol for Cooperating Ubiquitous Computing Devices	223
<i>Oliver Stannard and Frank Stajano</i>	
Am I in Good Company? A Privacy-Protecting Protocol for Cooperating Ubiquitous Computing Devices (Transcript of Discussion)	231
<i>Frank Stajano</i>	
Stayin' Alive: Aliveness as an Alternative to Authentication	242
<i>Jonathan Anderson and Robert N.M. Watson</i>	
Stayin' Alive: Aliveness as an Alternative to Authentication (Transcript of Discussion)	251
<i>Jonathan Anderson</i>	

Paul Revere Protocols 259
Paul Syverson

Paul Revere Protocols (Transcript of Discussion) 267
Paul Syverson

The Last Word 276

Author Index 277