Lecture Notes in Computer Science 7622

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

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

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 Klimaszewska 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	*in preparation*
17th Workshop (2009)	LNCS 7028	*in press*
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