Lecture Notes in Computer Science 5964

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

15th International Workshop
Brno, Czech Republic, April 18-20, 2007
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
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

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 Klimaszewska 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