Lecture Notes in Computer Science 2629

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Ali E. Abdallah
Peter Ryan
Steve Schneider (Eds.)

Formal Aspects of Security

First International Conference, FASec 2002
London, UK, December 16-18, 2002
Revised Papers

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Ali E. Abdallah
London South Bank University
School of Computing, Information Systems and Mathematics
Centre of Applied Formal Methods
Southwark Campus, 103 Borough Road, London, SE1 0AA, UK
E-mail: A.Abdallah@lsbu.ac.uk

Peter Ryan
University of Newcastle upon Tyne
School of Computing Science
Newcastle upon Tyne, NE1 7RU, UK
E-mail: peter.ryan@ncl.ac.uk

Steve Schneider
Royal Holloway, University of London
Department of Computer Science
Egham, Surrey, TW20 0EX, UK
E-mail: steve@cs.rhul.ac.uk

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

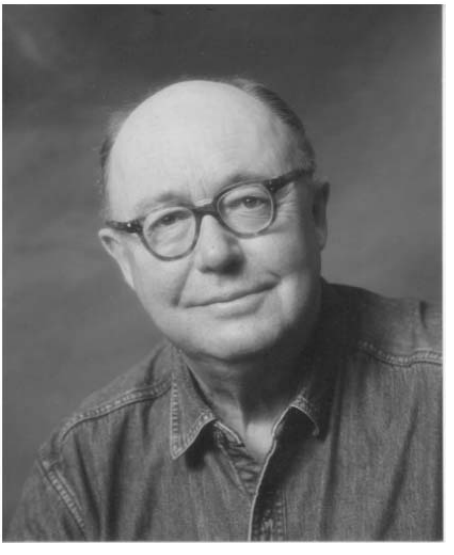
Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3, D.4.6, C.2.0, D.2.4, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-20693-0 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10975541 06/3142 5 4 3 2 1 0

This Proceedings Volume Is Dedicated to the Memory of Roger Needham



Roger was to have been one of the two keynote speakers at FASec. A few weeks before the event we heard that Roger was indisposed and would not be able to attend. A little later we learnt the sad news that Roger had in fact been diagnosed with terminal cancer and then, in March, that he had passed away. We have decided to dedicate these proceedings to his memory.

Roger was very much a "Cambridge Man." Doing his first degree at Cambridge, followed by a Ph.D., he then went on to become a professor in 1981 and Head of the Computer Laboratory from 1980 until 1995.

Roger was one of the outstanding pioneers of the field of computer science, being one of the driving forces behind the Cambridge Ring, the Cambridge Model Distributed System, and the UNIVERSE project.

He was also responsible for a number of seminal contributions in the field of computer security. He introduced the idea of storing the cryptographic hashes of passwords. He co-invented authentication protocols with Schroeder. He was also a co-author, with Burrows and Abadi, of the seminal BAN logic, the first rigorous framework for the analysis of cryptographic security protocols.

In 1997 Roger was lured away from the Computer Laboratory to set up Microsoft Research in Cambridge. This brought together many of the best researchers in computer science and information security.

He was a Fellow of the Royal Society, the Royal Academy of Engineering and the British Computer Society. In 1998, Roger was awarded the IEE Faraday Medal.

His insight, vision and humanity will be missed by all of us.

Preface

Formal Aspects of Security (FASec) was held at Royal Holloway, University of London, 18–20 December 2002. The occasion celebrated a Jubilee, namely the 25th anniversary of the establishment of BCS-FACS, the Formal Aspects of Computing Science specialist group of the British Computer Society. FASec is one of a series of events organized by BCS-FACS to highlight the use of formal methods, emphasize their relevance to modern computing, and promote their wider application. As the architecture model of information systems evolves from unconnected PCs, through intranet (LAN) and internet (WAN), to mobile internet and grids, security becomes increasingly critical to all walks of society: commerce, finance, health, transport, defence and science. It is no surprise therefore that security is one of the fastest-growing research areas in computer science.

The audience of FASec includes those in the formal methods community who have (or would like to develop) a deeper interest in security, and those in security who would like to understand how formal methods can make important contributions to some aspects of security. The scope of FASec is deliberately broad and covers topics that range from modelling security requirements through specification, analysis, and verifications of cryptographic protocols to certified code. The discussions at FASec 2002 encompassed many aspects of security: from theoretical foundations through support tools and on to applications. Formal methods has made a substantial contribution to this exciting field in the past. Our intended keynote speaker, Prof. Roger Needham, to whom this proceedings volume is dedicated, was one of the first researchers to mention, almost 25 years ago, that formal methods could be useful for assuring the correctness of security protocols [Needham and Schroeder, Using encryption for authentication in large networks of computers, CACM, 1978]. Judging by the quality of the papers in this volume, formal methods promise to make significant contributions to security in the future.

We were very privileged to include in the conference program contributions from a number of outstanding international invited speakers:

Fred Schneider	Cornell University, USA
Ernie Cohen	Microsoft Research, UK
Dieter Gollmann	Microsoft Research, UK
Andy Gordon	Microsoft Research, UK
Lawrence Paulson	University of Cambridge, UK
Bart Preneel	Catholic University of Leuven, Belgium
Susan Stepney	University of York, UK

Our gratitude goes to the authors for submitting their papers and responding to the feedback provided by the referees. Our thanks go to the referees for their valuable efforts in providing detailed and timely reviews of the papers. We owe special thanks to the BCS-FACS steering committee and its chairman, Jonathan P. Bowen, for their solid support of this event. Special thanks are also due for the generous contributions of our sponsors: MSR (Microsoft Research), CSR (Centre for Software Reliability), Adelard, and DSTL (Defence Science and Technology Laboratory). Finally, we are very grateful to the local organization team, especially to Janet Hales, for their professionalism and hard work, which ensured the smooth running of the local arrangements.

Online information concerning the conference is available at
http://www.lsbu.ac.uk/menass/fasec
or from the BCS-FACS Web site:
http://www.bcs-facs.org

FASec attracted more than sixty participants from the UK, Europe, USA, Canada, and Australia. The audience comprised a unique mixture of participants from different backgrounds and organizations (industrial and academic). The program contained an interesting combination of exciting topics in invited and refereed talks. These factors, combined with the charm of the Royal Holloway venue, the bright sun for the whole duration of the conference (yes, unbelievable, pleasant December English weather!), and a wonderful after-dinner speech by Tom Anderson (CSR) in the beautiful surroundings of the famous Picture Gallery, greatly helped in making FASec a memorable, intellectually stimulating, lively, and enjoyable event. We hope this proceedings captures some of the spirit of this event.

London and Newcastle, March 2003

Ali Abdallah, Peter Ryan
and Steve Schneider

Organization

Program Committee

Ali Abdallah	London South Bank University, UK (*Conference Co-chair*)
Jonathan Bowen	London South Bank University, UK (*BCS-FACS Chair*)
John Cooke	Loughborough University, UK
Neil Evans	Royal Holloway, University of London, UK
Cedric Fournet	Microsoft Research, UK
Dieter Gollmann	Microsoft Research, UK
Jeremy Jacob	University of York, UK
Wenbo Mao	HP Labs, UK
Lawrence Paulson	University of Cambridge, UK
Peter Ryan	University of Newcastle, UK (*Conference Co-chair*)
Steve Schneider	Royal Holloway, University of London, UK (*Conference Co-chair*)

Local Organizers

Neil Evans	Royal Holloway, University of London, UK
Mark Green	Oxford Brookes University, UK
Janet Hales	Royal Holloway, University of London, UK
Etienne Khayat	London South Bank University, UK
Steve Schneider	Royal Holloway, University of London, UK

Sponsors

Table of Contents

Security Modelling and Reasonning

Invited Talks III

Intrusion Detection Systems and Liveness