Lecture Notes in Computer Science 2437
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

George Davida Yair Frankel
Owen Rees (Eds.)

Infrastructure Security

International Conference, InfraSec 2002
Bristol, UK, October 1-3, 2002
Proceedings

Springer

Series Editors

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

Volume Editors

George Davida
University of Wisconsin-Milwaukee
Milwaukee, WI 53201, USA
E-mail: davida@cs.uwm.edu

Yair Frankel
TechTegrity LLC
P.O. Box 2125, Westfield, NJ 07091, USA
E-mail: yfrankel@cryptographers.com

Owen Rees
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol, BS34 8QZ, UK
E-mail: owen.rees@hp.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Infrastructure security : international conference ; proceedings / InfraSec 2002, Bristol, UK, October 1 - 3, 2002. George Davida .... - Berlin ; Heidelberg ; New York ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2437)
ISBN 3-540-44309-6

CR Subject Classification (1998): D.4.6, C.2.9, D.2, E.3, H.2.0, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-44309-6 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e. K.
Printed on acid-free paper SPIN 10870164 06/3142 5 4 3 2 1 0

Preface

Infrastructure Security Conference 2002 (InfraSec 2002) was created to promote security research and the development of practical solutions in the security of infrastructures – both government and commercial – such as the effective prevention of, detection of, reporting of, response to and recovery from security incidents. The conference, sponsored by the Datacard Group and Hewlett-Packard Laboratories, was held on October 1–3, 2002. Organizational support was provided by the Center for Cryptography, Computer and Network Security Center at the University of Wisconsin-Milwaukee.

Organizing a conference is a major undertaking requiring the efforts of many individuals. The Conference President, Graham Higgins (Datacard Group), oversaw all arrangements for the conference, and the General Chair, Susan Thompson (Datacard Group), oversaw the local organization and registration. Local arrangements were directed by Jan Ward (Hewlett-Packard Laboratories) and Jamie Wilson (Datacard Group). Financial arrangements were managed by Natalie Churchill (Hewlett-Packard Laboratories). We wish to thank the organizers, without whose support this conference would not have been possible.

This conference program included two keynote speakers: Bob Evans (Office of the e-Envoy) and Vic Maconachy (Department of Defense). The program committee considered 44 submissions of which 23 papers were accepted. Each submitted paper was reviewed by a minimum of three referees. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the content of their papers.

We thank all the authors who submitted to the conference, without which it would not have been successful. Our thanks to the program committee and all reviewers.

July 2002 George Davida, Yair Frankel, Owen Rees

Infrastructure Security 2002

October 1–3, Bristol, UK

Sponsored by

Datacard Group
Hewlett-Packard Laboratories

Conference President
Graham Higgins, Datacard Group

General Chair
Susan Thompson, Datacard Group

Program Chair
George Davida, University of Wisconsin-Milwaukee

Program Co-chairs
Yair Frankel, TechTegrity LLC
Owen Rees, Hewlett-Packard Laboratories

Program Committee

Alan Borrett ..... CESG
Don Beaver .....Seagate Research
Elisa Bertino .....Universita' di Milano
Bob Blakley .....IBM
Matt Blaze..... AT&T
Giovanni DiCrescenzo ..... Telcordia
David Everett .....Microexpert
Sigrid Gürgens ..... GMD
Cynthia Irvine ..... Naval Postgraduate School
Javier Lopez.....University of Malaga
Masahiro Mambo..... Tohoku University
Wembo Mao .....Hewlett-Packard Laboratories
Rene Peralta..... Yale University
Matt Robshaw..... Royal Holloway, University of London
Kazue Sako ..... NEC
Colin Walter.....Comodo Group

Table of Contents

Vulnerability Assessment and Logs

System Design

Formal Methods

Cryptographic Techniques

Networks