

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

2437

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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

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

Biometrics

Biometric Authentication in Infrastructure Security	1
<i>John Armington, Purdy Ho, Paul Koznek, Richard Martinez</i>	
Denial of Access in Biometrics-Based Authentication Systems	19
<i>Luciano Rila</i>	

Identification, Authentication, and Process

A Novel Approach to Proactive Password Checking	30
<i>Carlo Blundo, Paolo D'Arco, Alfredo De Santis, Clemente Galdi</i>	
Single Sign-On Architectures	40
<i>Jan De Clercq</i>	
Active Digital Credentials: Dynamic Provision of Up-to-Date Identity Information	59
<i>Marco Casassa Mont, Richard Brown</i>	

Analysis Process

How to Buy Better Testing (Using Competition to Get the Most Security and Robustness for Your Dollar)	73
<i>Stuart Schechter</i>	
Structured Risk Analysis	88
<i>Neil McEvoy, Andrew Whitcombe</i>	
A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls	104
<i>E.S. Siougle, V.C. Zorkadis</i>	

Mobile Networks

Authentication and Authorization of Mobile Clients in Public Data Networks	115
<i>Prakash Reddy, Venky Krishnan, Kan Zhang, Devaraj Das</i>	
A Contemporary Foreword on GSM Security	129
<i>Paulo S. Pagliusi</i>	

Vulnerability Assessment and Logs

Vulnerability Assessment Simulation for Information Infrastructure Protection.....	145
<i>HyungJong Kim, KyungHee Koh, DongHoon Shin, HongGeun Kim</i>	
Pseudonymizing Unix Log Files.	162
<i>Ulrich Flegel</i>	

System Design

DPS: An Architectural Style for Development of Secure Software	180
<i>Pascal Fenkam, Harald Gall, Mehdi Jazayeri, Christopher Kruegel</i>	
A New Infrastructure for User Tracking Prevention and Privacy Protection in Internet Shopping.....	199
<i>Matthias Enzmann, Thomas Kunz, Markus Schneider</i>	
Different Smartcard-Based Approaches to Physical Access Control	214
<i>Óscar Cánovas, Antonio F. Gómez, Humberto Martínez, Gregorio Martínez</i>	

Formal Methods

Authenticity and Provability – A Formal Framework	227
<i>Sigrid Gürgens, Peter Ochsenschläger, Carsten Rudolph</i>	
Protocol Engineering Applied to Formal Analysis of Security Systems	246
<i>Javier Lopez, Juan J. Ortega, Jose M. Troya</i>	

Cryptographic Techniques

Applications of Multiple Trust Authorities in Pairing Based Cryptosystems.....	260
<i>L. Chen, K. Harrison, D. Soldera, N.P. Smart</i>	
Plausible Deniability Using Automated Linguistic Stegonagraphy	276
<i>Mark Chapman, George Davida</i>	
Virtual Software Tokens – A Practical Way to Secure PKI Roaming	288
<i>Taekyoung Kwon</i>	
Bit-Serial AOP Arithmetic Architectures over $GF(2^m)$	303
<i>Hyun-Sung Kim, Kee-Young Yoo</i>	

Networks

A Practical Distributed Authorization System for GARA	314
<i>William A. Adamson, Olga Kornievskaia</i>	

Design of a VPN Software Solution Integrating TCP and UDP Services ...	325
<i>Javier Lopez, Jose A. Montenegro, Rodrigo Roman, Jorge Davila</i>	

Author Index	339
---------------------------	-----