Lecture Notes in Computer Science 2820

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Giovanni Vigna Erland Jonsson
Christopher Kruegel (Eds.)

Recent Advances in Intrusion Detection

6th International Symposium, RAID 2003
Pittsburgh, PA, USA, September 8-10, 2003
Proceedings

Springer

Volume Editors

Giovanni Vigna
Christopher Kruegel
University of California, Santa Barbara, Department of Computer Science
Santa Barbara, CA 93106, USA
E-mail: {vigna, chris}@cs.ucsb.edu

Erland Jonsson
Chalmers University of Technology, Department of Computer Engineering
41296 Goteborg, Sweden
E-mail: erland.jonsson@ce.chalmers.se

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 Nationalbibliographie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): K.6.5, K.4, E.3, C.2, D.4.6

ISSN 0302-9743
ISBN 3-540-40878-9 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10953587 06/3142 5 4 3 2 1 0

Preface

On behalf of the Program Committee, it is our pleasure to present to you the proceedings of the Sixth Symposium on Recent Advances in Intrusion Detection (RAID 2003).

The program committee received 44 full paper submissions from 10 countries. All submissions were carefully reviewed by at least three program committee members or additional intrusion detection experts according to the criteria of scientific novelty, importance to the field, and technical quality. The program committee meeting was held in Berkeley, USA on May 14–15. Thirteen papers were selected for presentation and publication in the conference proceedings.

The conference technical program included both fundamental research and practical issues, and was shaped around the following topics: network infrastructure, anomaly detection, correlation, modeling and specification, and sensor technologies.

The slides presented by the authors are available on the RAID 2003 web site, http://www.raid-symposium.org/raid2003.

We would like to thank the authors that submitted papers as well as the program committee members and the additional reviewers who volunteered their time to create a quality program. In addition, we want to thank the Conference General Chair, John McHugh, for organizing the conference in Pittsburgh, Joshua Haines for publicizing the conference, Don McGillen for finding support from our sponsors, and Christopher Kruegel for maintaining the RAID web site and preparing the conference proceedings.

Special thanks go to our sponsors Cisco Systems and Symantec, who provided financial support for student participation to the symposium, and to CERT/CMU for hosting the conference.

September 2003

Giovanni Vigna
Erland Jonsson

Organization

RAID 2003 was organized by and gratefully acknowledges the support of the Center for Computer and Communications Security at Carnegie Mellon University and the CERT Coordination Center.

Conference Chairs

General Chair:	John McHugh (CERT/SEI, Carnegie Mellon University, USA)
Program Chairs:	Giovanni Vigna (UC Santa Barbara, USA) Erland Jonsson (Chalmers University of Technology, Sweden)
Publication Chair:	Christopher Kruegel (UC Santa Barbara, USA)
Publicity Chair:	Joshua Haines (MIT Lincoln Laboratory, USA)
Sponsor Chair:	Don McGillen (Carnegie Mellon University, USA)

Program Committee

Marc Dacier	Eurecom, France
Hervé Debar	France Telecom R&D, France
Joshua Haines	MIT Lincoln Laboratory, USA
Dick Kemmerer	UC Santa Barbara, USA
Calvin Ko	Network Associates Inc., USA
Christopher Kruegel	UC Santa Barbara, USA
Wenke Lee	Georgia Institute of Technology, USA
Ulf Lindqvist	SRI, USA
Roy Maxion	Carnegie Mellon University, USA
Ludovic Mé	Supélec, France
Vern Paxson	ACIRI/LBNL, USA
Phil Porras	SRI, USA
Rama Sekar	SUNY Stony Brook, USA
Stuart Staniford	Silicon Defense, USA
Kymie Tan	Melbourne University, Australia
Al Valdes	SRI, USA
Andreas Wespi	IBM Research, Switzerland
S. Felix Wu	UC Davis, USA
Diego Zamboni	IBM Research, Switzerland

Steering Committee

Marc Dacier (Chair)	Eurecom, France
Hervé Debar	France Telecom R&D, France
Deborah Frincke	University of Idaho, USA
Ming-Yuh Huang	The Boeing Company, USA
Wenke Lee	Georgia Institute of Technology, USA
Ludovic Mé	Supélec, France
S. Felix Wu	UC Davis, USA
Andreas Wespi	IBM Research, Switzerland
Giovanni Vigna	UC Santa Barbara, USA

Additional Reviewers

Dominique Alessandri	IBM Zurich Research Laboratory, Switzerland
Magnus Almgren	Chalmers University of Technology, Sweden
Sandeep Bhatkar	SUNY Stony Brook, USA
Ramesh Govindan	University of Southern California, USA
Jeffery Hansen	Carnegie Mellon University, USA
Klaus Julisch	IBM Zurich Research Laboratory, Switzerland
Kevin Killourhy	Carnegie Mellon University, USA
Zhenkai Liang	SUNY Stony Brook, USA
Emilie Lundin	Chalmers University of Technology, Sweden
Darren Mutz	UC Santa Barbara, USA
Fabien Pouget	Eurecom, France
William Robertson	UC Santa Barbara, USA
Umesh Shankar	University of California, Berkeley, USA
Prem Uppuluri	SUNY Stony Brook, USA
Fredrik Valeur	UC Santa Barbara, USA
V. Venkatakrishnan	SUNY Stony Brook, USA
Wei Xu	SUNY Stony Brook, USA

Table of Contents

Anomaly Detection II