Lecture Notes in Computer Science 2212
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Wenke Lee Ludovic Mé Andreas Wespi (Eds.)

Recent Advances in Intrusion Detection

4th International Symposium, RAID 2001
Davis, CA, USA, October 10-12, 2001
Proceedings

Springer

Volume Editors

Wenke Lee
Georgia Institute of Technology, College of Computing
801 Atlantic Drive, Atlanta, Georgia 30332-0280, USA
E-mail: wenke@cc.gatech.edu

Ludovic Mé
SUPELEC
BP 28, 35511 Cesson Sevigne Cedex, France
E-mail: Ludovic.Me@supelec.fr

Andreas Wespi
IBM Research, Zurich Research Laboratory
Säumerstr. 4, 8803 Rüschlikon, Switzerland
E-mail: anw@zurich.ibm.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Recent advances in intrusion detection : 4th international symposium ;
proceedings / RAID 2001, Davis, CA, USA, October 10 - 12, 2001.
Wenke Lee ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2212)
ISBN 3-540-42702-3

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

ISSN 0302-9743
ISBN 3-540-42702-3 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 PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10840834 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 fourth Recent Advances in Intrusion Detection Symposium.

The RAID 2001 program committee received 55 paper submissions from 13 countries. All submissions were carefully reviewed by several members of the program committee on the criteria of scientific novelty, importance to the field, and technical quality. Final selection took place at a meeting held on May 16-17 in Oakland, California. Twelve papers were selected for presentation and publication in the conference proceedings. In addition, nine papers, presenting work in progress, were selected for presentation.

The program included both fundamental research and practical issues: logging and IDS integration, attack modeling, anomaly detection, specification-based IDS, IDS assessment, IDS cooperation, intrusion tolerance, and legal aspects.

RAID 2001 also hosted two panels, one on "The Present and Future of IDS Testing Methodologies," a subject of major concern for all IDS users and designers, and one on "Intrusion Tolerance," an emerging research area of increasing importance.

Dr. Bill Hancock, Senior Vice President and Chief Security Officer of Exodus Communications, Inc., delivered a keynote speech "Real world intrusion detection or how not to become a deer in the headlights of an attacker's car on the information superhighway".

The slides presented by the authors, the 9 papers which are not in the proceedings, and the slides presented by the panelists are available on the website of the RAID symposium series, `http://www.raid-symposium.org/`.

We would like to thank all authors who submitted papers, as well as the program committee members and the additional reviewers, for their efforts. Special thanks go to Felix Wu for handling the conference arrangements, Niranjan Balwalli for maintaining the paper submission Web site, Giovanni Vigna for publicizing the conference, and Andreas Wespi for maintaining the RAID Web pages and preparing the conference proceedings. Finally, we thank all the RAID 2001 sponsors.

October 2001

Ludovic Mé
Wenke Lee

Organization

RAID 2001 was hosted by and gratefully acknowledges the support of the University of California at Davis, CA.

Conference Chairs

Executive Committee Chair:	Marc Dacier (IBM Research, Switzerland)
Program Co-chairs:	Ludovic Mé (Supélec, France)
	Wenke Lee (Georgia Institute of Technology, USA)
Publication Chair:	Andreas Wespi (IBM Research, Switzerland)
Local Organization Chair:	S. Felix Wu (UC Davis, USA)
Publicity Chair:	Giovanni Vigna (UC Santa Barbara, USA)

Program Committee

Matt Bishop	UC Davis, USA
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	ONERA, France
Marc Dacier	IBM Research, Switzerland
Hervé Debar	France Télécom R&D, France
Yves Deswarte	LAAS-CNRS, France
Deborah Frincke	University of Idaho, USA
Anup Ghosh	Cigital, USA
Tim Grance	NIST, USA
Ming-Yuh Huang	Boeing Applied Research and Technology, USA
Erland Jonsson	Chalmers University of Technology, Sweden
Richard Kemmerer	UC Santa Barbara, USA
Calvin Ko	Network Associates, USA
Baudouin Le Charlier	Université de Namur, Belgium
Wenke Lee	Georgia Institute of Technology, USA
Richard Lippmann	MIT Lincoln Laboratory, USA
John McHugh	CERT/SEI, Carnegie Mellon University, USA
Roy Maxion	Carnegie Mellon University, USA
George Mohay	Queensland University, Australia
Ludovic Mé	Supélec, France
Abdelaziz Mounji	Swift, Belgium
Vern Paxson	ACIRI/LBNL, USA
Phil Porras	SRI, USA
Stuart Staniford	Silicon Defense, USA
Al Valdes	SRI, USA
Giovanni Vigna	UC Santa Barbara, USA

Andreas Wespi	IBM Research, Switzerland
S. Felix Wu	UC Davis, USA
Diego Zamboni	Purdue University, USA
Kevin Ziese	Cisco Systems, USA

Additional Reviewers

Magnus Almgren	SRI, USA
Phillip Attfield	Boeing Applied Research and Technology, USA
Salem Benferhat	IRIT, Université Paul Sabatier, France
Paul Brutch	Network Associates, USA
Steven Cheung	SRI, USA
Ulrich Flegel	University of Dortmund, Germany
Frank Hill	Cigital, Inc., USA
Klaus Julisch	IBM Research, Switzerland
Vincent Letocart	Université de Namur, Belgium
Emilie Lundin	Chalmers University of Technology, Sweden
Donald Marks	NIST, USA
Peter Mell	NIST, USA
Matt Schmid	Cigital, USA
Kymie M.C. Tan	Carnegie Mellon University, USA

Table of Contents

Legal Aspects

Specification-Based IDS