Lecture Notes in Computer Science 1907

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

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

Hervé Debar Ludovic Mé
S. Felix Wu (Eds.)

Recent Advances in Intrusion Detection

Third International Workshop, RAID 2000
Toulouse, France, October 2-4, 2000
Proceedings

Springer

Series Editors

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

Volume Editors

Hervé Debar
France Télécom R & D
42 Rue des Coutoures, 14000 Caen, France
E-mail: herve.debar@francetelecom.fr

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

S. Felix Wu
University of California at Davis
Department of Computer Science, 2063 Engineering II
One Shields Avenue, Davis, CA 95616-8562, USA
E-mail: wu@cs.ucdavis.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Recent advances in intrusion detection : third international workshop ;
proceedings / RAID 2000, Toulouse, France, October 2 - 4, 2000.
Hervé Debar . . . (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer,
2000
(Lecture notes in computer science ; Vol. 1907)
ISBN 3-540-41085-6

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

ISSN 0302-9743
ISBN 3-540-41085-6 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
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10722688 06/3142 5 4 3 2 1 0

Preface

Since 1998, RAID has established its reputation as the main event in research on intrusion detection, both in Europe and the United States. Every year, RAID gathers researchers, security vendors and security practitioners to listen to the most recent research results in the area as well as experiments and deployment issues.

This year, RAID has grown one step further to establish itself as a well-known event in the security community, with the publication of hardcopy proceedings. RAID 2000 received 26 paper submissions from 10 countries and 3 continents. The program committee selected 14 papers for publication and examined 6 of them for presentation. In addition RAID 2000 received 30 extended abstracts proposals; 15 of these extended abstracts were accepted for presentation. Extended abstracts are available on the website of the RAID symposium series, `http://www.raid-symposium.org/`. We would like to thank the technical program committee for the help we received in reviewing the papers, as well as all the authors for their participation and submissions, even for those rejected.

As in previous RAID symposiums, the program alternates between fundamental research issues, such as new technologies for intrusion detection, and more practical issues linked to the deployment and operation of intrusion detection systems in a real environment. Five sessions have been devoted to intrusion detection technology, including modeling, data mining and advanced techniques. Four sessions have been devoted to topics surrounding intrusion detection, such as evaluation, standardization and legal issues, logging and analysis of intrusion detection information. RAID will also host two panels, one on practical deployment of intrusion-detection systems where users of the technology will share their experience with the audience and one on the distributed denial of service attacks that generated a lot of attention in early 2000.

In summary, we hope that this very dense program and mix of practical and theoretical issues will satisfy the users of intrusion detection systems and encourage the researchers in the area to continue improving their technology.

October 2000

Hervé Debar
S. Felix Wu

Organization

RAID 2000 is hosted by and gratefully acknowledges the support of ONERA Centre de Toulouse.

Conference Chairs

Executive Committee Chair	Marc Dacier (IBM Research, Switzerland)
Program Co-Chairs	Hervé Debar (IBM Research, Switzerland)
	S. Felix Wu (North Carolina State University, USA)
Publication Chair	Ludovic Mé (Supélec, France)

Program Committee

Matt Bishop	University of California at Davis, USA
Dick Brackney	National Security Agency, USA
Rowena Chester	University of Tennessee, USA
Frédéric Cuppens	ONERA, France
Marc Dacier	IBM Research, Switzerland
Hervé Debar	IBM Research, Switzerland
Yves Deswarte	LAAS-CNRS and SRI-International, France
Terry Escamilla	IBM, USA
Deborah Frincke	University of Idaho, USA
Tim Grance	National Institute of Standards and Technology, USA
Ming-Yuh Huang	The Boeing Company, USA
Erland Jonsson	Chalmers University of Technology, Sweden
Sokratis Katsikas	University of the Aegean, Greece
Baudouin Le Charlier	Universite de Namur, Belgium
Ludovic Mé	Supélec, France
Abdelaziz Mounji	Swift, Belgium
Vern Paxson	ACIRI/LBNL, USA
Jean-Jacques Quisquater	Universite Catholique de Louvain, Belgium
Mark Schneider	National Security Agency, USA
Steve Smaha	Free Agent, USA
Peter Sommer	London School of Economics and Political Science, England
Stuart Staniford-Chen	Silicon Defense, USA
Peter Thorne	University of Melbourne, Australia
S. Felix Wu	North Carolina State University, USA
Kevin Ziese	Cisco Systems, USA

Additional Referees

Dominique Alessandri	IBM Research, Switzerland
Klaus Julisch	IBM Research, Switzerland
Andreas Wespi	IBM Research, Switzerland

Local Organization Committee

Frédéric Cuppens	ONERA, France
Claire Saurel	ONERA, France

Sponsoring Institutions

Alcatel
IBM
Internet Security Systems