Lecture Notes in Computer Science 4219

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Diego Zamboni Christopher Kruegel (Eds.)

Recent Advances in Intrusion Detection

9th International Symposium, RAID 2006
Hamburg, Germany, September 20-22, 2006
Proceedings

Springer

Volume Editors

Diego Zamboni
IBM Research GmbH
Zurich Research Laboratory
Säumerstr. 4, Postfach, 8803 Rüschlikon, Switzerland
E-mail: dza@zurich.ibm.com

Christopher Kruegel
Technical University of Vienna
Secure Systems Lab
Treitlstrasse 3, A-1040 Vienna, Austria
E-mail: chris@auto.tuwien.ac.at

Library of Congress Control Number: 2006932117

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-39723-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-39723-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11856214 06/3142 5 4 3 2 1 0

Preface

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 9th Symposium on Recent Advances in Intrusion Detection (RAID 2006), which took place in Hamburg, Germany, on September 20-22, 2006.

As every year since 1998, the symposium brought together leading researchers and practitioners from academia, government and industry to discuss intrusion detection research and practice. We had sessions on anomaly and specification-based detection, network-based intrusion detection, attacks against intrusion detection systems, IDS evaluation and malware analysis.

The RAID 2005 Program Committee received 93 paper submissions from all over the world, including 15 papers submitted as "Big Challenge, Big Idea" papers. All the submissions were carefully reviewed by several members of the Program Committee and evaluated on the basis of scientific novelty, importance to the field, and technical quality. Final selection took place at the Program Committee meeting held on June 1st and 2nd in Zürich, Switzerland. Sixteen papers were selected for presentation and publication in the conference proceedings, placing RAID among the most competitive conferences in the area of computer security.

This year we announced "Big Challenge, Big Idea" as a theme. We encouraged submissions in a separate category, looking for papers that described fundamental problems that have not yet been tackled by intrusion detection research, or bold, risky or controversial ideas for potential research or solutions.

A successful symposium is the result of the joint effort of many people. In particular, we would like to thank all the authors who submitted papers, whether accepted or not. We also thank the Program Committee members and additional reviewers for their hard work in evaluating the submissions. In addition, we want to thank the General Chair, Dieter Gollmann, for handling the conference arrangements, Robert Cunningham for publicizing the conference, James Riordan for putting together the conference proceedings, Klaus-Peter Kossakowski for finding sponsor support, and Jan Meier for maintaining the conference Web site. Finally, we extend our thanks to the Northwest Security Institute (NSWI) and Cisco Systems for their sponsorship of student scholarships.

September 2006

Diego Zamboni
Christopher Kruegel

Organization

RAID 2006 was organized by the Technical University of Hamburg-Harburg and held in conjunction with ESORICS 2006.

Conference Chairs

General Chairs	Dieter Gollmann (Technical University Hamburg-Harburg), Andreas Günter(HiTech)
Program Chair	Diego Zamboni (IBM Zurich Research Laboratory)
Program Co-chair	Christopher Kruegel (Technical University Vienna)
Publication Chair	James Riordan (IBM Zurich Research Laboratory)
Publicity Chair	Robert Cunningham (MIT Lincoln Laboratory)
Sponsorship Chair	Klaus-Peter Kossakowski (PRESECURE Consulting)

Program Committee

Magnus Almgren	Chalmers University, Sweden
Michael Behringer	Cisco Systems, Inc., USA
Sungdeok Cha	Korea Advanced Institute of Science and Technology, Korea
Steve J. Chapin	Systems Assurance Institute, Syracuse University, USA
Andrew Clark	Queensland University of Technology, Australia
Crispin Cowan	Novell, USA
Robert Cunningham	MIT Lincoln Laboratory, USA
Olivier De Vel	Department of Defence, Australia
Farnam Jahanian	University of Michigan and Arbor Networks, USA
Somesh Jha	University of Wisconsin, Madison, USA
Klaus-Peter Kossakowski	DFN-CERT, Germany
Christopher Kruegel	Technical University Vienna, Austria
Kwok-Yan Lam	Tsinghua University, China
Ulf Lindqvist	SRI International, USA
Raffael Marty	ArcSight, Inc., USA
George Mohay	Queensland University of Technology, Australia
Benjamin Morin	Supélec, France

Program Committee (Continued)

Peng Ning	North Carolina State University, USA
James Riordan	IBM Zurich Research Laboratory, Switzerland
Rei Safavi-Naini	University of Wollongong, Australia
Dawn Song	Carnegie Mellon University, USA
Sal Stolfo	Department of Computer Science, Columbia University, USA
Toshihiro Tabata	Okayama University, Japan
Kymie Tan	Carnegie Mellon University, USA
Vijay Varadharajan	Macquarie University, Australia
Giovanni Vigna	University of California at Santa Barbara, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Steering Committee

Marc Dacier (chair)	Eurecom, France
Hervé Debar	France Telecom R&D, France
Deborah Frincke	Pacific Northwest National Lab, USA
Ming-Yuh Huang	The Boeing Company, USA
Erland Jonsson	Chalmers, Sweden
Wenke Lee	Georgia Institute of Technology, USA
Ludovic Mé	Supélec, France
S. Felix Wu	UC Davis, USA
Andreas Wespi	IBM Research, Switzerland
Alfonso Valdes	SRI International, USA
Giovanni Vigna	UCSB, USA

Additional Reviewers

Hirotake Abe	Japan Science and Technology Agency, Japan
Stig Andersson	Queensland University of Technology, Australia
Mark Branagan	Queensland University of Technology, Australia
Hyung Chan Kim	Gwangju Institute of Science and Technology, Korea
Malcolm Corney	Queensland University of Technology, Australia
Siu-Leung Chung	Open University of Hong Kong
Gabriela F. Cretu	CS Department Columbia University, USA
Meng Ge	Tsinghua University, China
Daniel Hedin	Chalmers University of Technology and Göteborg University, Sweden

Additional Reviewers (Continued)

Matt Henricksen	Queensland University of Technology, Australia
Jeffrey Horton	University of Wollongong, Australia
Corrado Leita	Eurecom, France
Wei-Jen Li	CS Department Columbia University, USA
Zhuowei Li	Indiana University, USA
Liang Lu	University of Wollongong, Australia
Andreas Moser	Technical University Vienna
Yoshihiro Oyama	University of Electro-Communications, Japan
Janak Parekh	CS Department, Columbia University, USA
Van Hau Pham.	Eurecom, France
Bradley Schatz	Queensland University of Technology, Australia
Jinyang Shi	Tsinghua University, China
Hongwei Sun	Tsinghua University, China
Olivier Thonnard	Eurecom, France
Uday K. Tupakula	Macquarie University, Australia
Ke Wang	CS Department, Columbia University, USA
Jacob Zimmermann	Queensland University of Technology, Australia

Table of Contents

Malware Collection and Analysis

Anomaly- and Specification-Based Detection

Network Intrusion Detection