INTRUSION DETECTION IN DISTRIBUTED SYSTEMS

An Abstraction-Based Approach

Library of Congress Cataloging-in-Publication

ISBN 978-1-4613-5091-0 ISBN 978-1-4615-0467-2 (eBook)
DOI 10.1007/978-1-4615-0467-2

Originally published by Kluwer Academic Publishers in 2004
Softcover reprint of the hardcover 1st edition 2004

Printed on acid-free paper.

INTRUSION DETECTION IN DISTRIBUTED SYSTEMS

An Abstraction-Based Approach

by

Peng Ning
North Carolina State University, U.S.A.
Sushil Jajodia
George Mason University, U.S.A.
X. Sean Wang
University of Vermont, U.S.A.

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Advances in Information Security

Sushil Jajodia
Consulting editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers as well as developers are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1

DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4

SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1

APPLICATIONS OF DATA MINING IN COMPUTER SECURITY, edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3

MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1

TRUSTED RECOVERY AND DEFENSIVE INFORMATION WARFARE by Peng Liu and Sushil Jajodia, ISBN: 0-7923-7572-6

RECENT ADVANCES IN RSA CRYPTOGRAPHY by Stefan Katzenbeisser, ISBN: 0-7923-7438-X

E-COMMERCE SECURITY AND PRIVACY by Anup K. Ghosh, ISBN: 0-7923-7399-5

INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia, ISBN: 0-7923-7204-2

Additional information about this series can be obtained from
http://www.wkap.nl/prod/s/ADIS

To my grandma Huijun Wu,
and parents Changcheng
Ning and Kuiling Ao.
– PN

To my parents and my wife.
–SJ

To my children, with joy.
–XW

Contents

List of Figures

List of Tables

Preface

Intrusions in an information system are the activities that violate the security policy of the system, and *intrusion detection* is the process to identify intrusions. Intrusion detection has been studied for over 20 years. It is based on the beliefs that an intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized actions will be detectable.

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. Intrusion detection complements the protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusion attempts have happened or are happening, so that the users can understand the security threats and risks, and thus be better prepared for future attacks.

Intrusion detection techniques are traditionally categorized into two classes: *anomaly detection* and *misuse detection.* Anomaly detection is based on the normal behavior of a subject (e.g., a user or a system); any action that significantly deviates from the normal behavior is considered intrusive. Misuse detection catches intrusions in terms of the characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of a known attack or vulnerability is considered intrusive.

Alternatively, IDSs may be classified into host-based IDSs, distributed IDSs, and network-based IDSs according to the sources of the audit information used by each IDS. Host-based IDSs get audit data from host audit trails, usually aiming at detecting attacks against a single host; distributed IDSs gather audit data from multiple hosts and possibly the network that connects the hosts, aiming at detecting attacks involving multiple hosts; network-based IDSs use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services.

This monograph presents the research contributions in three areas with respect to intrusion detection in distributed systems. The first contribution is an abstraction-based approach to addressing heterogeneity and autonomy of distributed environments. Specifically, the concept of *system view* is introduced to provide an abstract interface between different systems. On the one hand, system views hide the difference between heterogeneous systems; on the other hand, they describe what information an autonomous system is willing to provide to other systems.

The second contribution is a formal framework for modeling requests among cooperative IDSs and its application to Common Intrusion Detection Framework (CIDF). The first problem is how to enable IDSs to request specific information from other IDSs. To address this problem, the proposed technique represents a request to an IDS as a pattern plus a transformation rule, where the pattern specifies the events that the requesting party is interested in and the transformation rule extracts interesting information from the events. The formal approach is also used to add a query facility to the Common Intrusion Detection Framework (CIDF), which allows an IDS to form flexible requests to other systems.

The third contribution is a novel approach to coordinating different IDSs for distributed event correlation. The proposed technique represents the event correlation to be performed as a pattern (called a *signature*) among distributed events. A decentralized method is then presented for autonomous but cooperative IDSs to perform the event correlation specified by signatures. Specifically, a signature is decomposed into finer units called *detection tasks*, each of which represents the activity to be monitored in one place. The IDSs (involved in a signature) then perform the detection tasks cooperatively according to the "dependency" relationships among these tasks. Our approach is superior to the existing centralized or hierarchical approaches in that (1) communication is more efficient by having different IDSs communicate with each other only when necessary and (2) no centralized or hierarchical trust is required. As an important application of distributed event correlation, this approach can be used to represent and detect distributed (or coordinated) attacks that cannot be detected from a single place. An experimental system called CARDS has been implemented to test the feasibility of the proposed approaches.

PENG NING, SUSHIL JAJODIA, AND X. SEAN WANG

Acknowledgments

We are grateful to Joe Giordano of the Air Force Research Laboratory/Rome, David Hislop of the Army Research Office, and Maria Zemankova of the National Science Foundation for sponsoring our research presented in this volume.

It is also a pleasure to acknowledge the Association for Computing Machinery for allowing us to use material from "Abstraction-based intrusion detection in distributed environments," *ACM Transactions on Information and System Security*, Vol. 4, No. 4, November 2001, pages 407–452, and Elsevier Science for permission to use material from "Modeling requests among cooperating intrusion detection systems," *Computer Communications*, Vol. 23, No. 17, November 2000, pages 1702–1715, and "Design and Implementation of A Decentralized Prototype System for Detecting Distributed Attacks," *Computer Communications*, Vol. 25, No. 15, September 2002, pages 1374–1391.

Series Foreword

ADVANCES IN INFORMATION SECURITY

Sushil Jajodia
Consulting Editor

Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444

email: jajodia@gmu.edu

Welcome to the ninth volume of the Kluwer International Series on ADVANCES IN INFORMATION SECURITY. The goals of this series are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

The success of this series depends on contributions by researchers and developers such as you. If you have an idea for a book that is appropriate for this series, I encourage you to contact me. I would be happy to discuss any potential projects with you. Additional information about this series can be obtained from www.wkap.nl/series.htm/ADIS.

SUSHIL JAJODIA
Consulting Editor