DISSEMINATING SECURITY UPDATES AT INTERNET SCALE

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
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 www.wkap.nl/series.htm/ADIS.

DISSEMINATING SECURITY UPDATES AT INTERNET SCALE

by

Jun Li
University of Oregon

Peter Reiher
University of California, Los Angeles

Gerald J. Popek
University of California, Los Angeles
United Online

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Li, Jun; Reiher, Peter; Popek, Gerald J.
Disseminating Security Updates at Internet Scale

ISBN 978-1-4613-5355-3 ISBN 978-1-4615-1021-5 (eBook)
DOI 10.1007/978-1-4615-1021-5

Printed on acid-free paper.

To my parents
Tianyun Li and Cuiping Ma

Contents

List of Figures and Tables

Figures

Tables

Trademarks

Linux is a trademark of Linus Torvalds. Red Hat is a trademark of Red Hat Software, Inc. Java is a trademark of Sun Microsystems, Inc. AMD is a trademark of Advanced Micro Devices, Inc. Ethernet is a trademark of Xerox Corporation. CERT and CERT Coordination Center are trademarks of Carnegie Mellon University. BBC is a trademark of the British Broadcasting Corporation. VERISIGN is a trademark licensed to VeriSign, Inc. MICROSOFT and WINDOWS are trademarks of Microsoft Corporation. KERBEROS is a trademark of the Massachusetts Institute of Technology. RSA is a trademark of RSA Security Inc. iBEAM Broadcasting is a trademark of iBEAM Broadcasting Corporation. CacheWare is a trademark of CacheWare, Inc. Digital Island is a trademark of Digital Island, Inc. epicRealm is a trademark of epicRealm Operating Inc. PointCast is a trademark of PointCast, Inc. Xerox is a trademark of Xerox Corporation. BackWeb is a trademark of BackWeb Technologies. iFusion is a trademark of iFusion, LLC. McAfee is a trademark of Network Associates, Inc. Symantec is a trademark of Symantec Corporation. Ricochet is a trademark of Metricom, Inc.

Preface

Rapid and widespread dissemination of security updates throughout the Internet would be invaluable for many purposes, including sending early-warning signals, distributing new virus signatures, updating certificate revocation lists, dispatching event information for intrusion detection systems, etc. However, notifying a large number of machines securely, quickly, and with high assurance is very challenging. Such a system must compete with the propagation of threats, handle complexities in large-scale environments, address interruption attacks toward dissemination, and also secure itself.

Revere addresses these problems by building a large-scale, self-organizing and resilient overlay network on top of the Internet. This book describes Revere, and discusses how to secure the dissemination procedure and the overlay network, considering possible attacks and countermeasures. It further presents experimental measurements of a prototype implementation of Revere gathered using a large-scale-oriented approach. These measurements suggest that Revere can deliver security updates at the required scale, speed and resiliency for a reasonable cost.

This book describes methods to obtain practical, yet meaningful, performance results on systems that are designed to operate at scales too high to allow standard experiments. While simulations can offer some insights into aspects of large-scale systems, the hybrid approaches used to measure Revere can give more realistic results, since they typically rely on execution of real code with real background operations.

Finally, this book will be helpful to those trying to design peer systems at large scale when security is a concern, since many of the issues faced by these designs are also faced by Revere. The Revere solutions may not always be appropriate for other peer systems with very different goals, but the analysis of the problems and possible solutions discussed here will be helpful in designing a customized approach for such systems.

Acknowledgments

Frequent interactions with our colleagues at the Laboratory for Advanced Systems Research, University of California, Los Angeles, greatly enhanced the quality and experience of this research. We thank all members of this group, but give special thanks to Dr. Geoff Kuenning for his help in presenting this research, Dr. Mark Yarvis for sharing his thoughts on writing a good technical book, Scott Michel for his willingness to test Revere, and Arnell Pablo for setting up testbed machines.

Janice Wheeler greatly improved the clarity and elegance of this book. We are indebted to her, both for her expert editing work and for always being there when needed.

Special permission to reproduce "CERT Advisory CA-2001-23 Figure 1," copyright © 2001 by Carnegie Mellon University, is granted by the Software Engineering Institute. Thanks also go to CAIDA for providing the figure on the patching rate of machines infected by the CodeRed Worm.