
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 Kırılı, 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

Copyright © 2003 by Springer Science+Business Media New York
Originally published by Kluwer Academic Publishers in 2003
Softcover reprint of the hardcover 1st edition 2003

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording, or otherwise, without the written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

Permission for books published in Europe: permissions@wkap.nl
Permissions for books published in the United States of America: permissions@wkap.com

Printed on acid-free paper.

To my parents
Tianyun Li and Cuiping Ma

Contents

| | |
|-------------------------------------------------------------------|-------------|
| List of Figures and Tables | ix |
| Trademarks | xi |
| Preface..... | xiii |
| Acknowledgments | xv |
| 1. Introduction | 1 |
| 1.1 Case Studies | 1 |
| 1.2 Goal of Revere | 6 |
| 1.3 Assumptions | 7 |
| 1.4 Challenges | 8 |
| 1.5 Revere Overview | 9 |
| 1.6 Key Contributions of This Research | 10 |
| 1.7 Roadmap of This Book | 11 |
| 2. Assurance via Redundancy | 13 |
| 2.1 The Redundancy Approach | 13 |
| 2.2 Interruption Threats | 15 |
| 2.3 Transmission Primitives | 16 |
| 2.4 Assurance via Redundancy | 18 |
| 2.5 Employing Redundancy in Revere | 20 |
| 2.6 Conclusions | 21 |
| 3. RBone: A Self-Organized Resilient Overlay Network | 23 |
| 3.1 Principles for Building an RBone | 24 |
| 3.2 RBone Formation | 28 |
| 3.3 Adaptive Management of RBone | 38 |
| 3.4 Messages and Data Structures | 39 |
| 3.5 Building a Common RBone | 43 |
| 3.6 Conclusions | 46 |
| 4. Dissemination Procedure | 47 |
| 4.1 Dissemination Principle | 47 |
| 4.2 Dissemination Center | 49 |
| 4.3 Security Update Format | 50 |
| 4.4 Pushing: A Store-And-Forward Mechanism | 50 |

| | |
|--------------------------------------------------------|------------|
| 4.5 Pulling Security Updates | 60 |
| 4.6 Open Issues | 64 |
| 4.7 Conclusions | 65 |
| 5. Security | 67 |
| 5.1 Assumptions | 67 |
| 5.2 Security of Dissemination Procedure | 68 |
| 5.3 Securely Building and Maintaining RBones | 80 |
| 5.4 Attacks and Countermeasures | 87 |
| 5.5 Open Issues | 90 |
| 5.6 Conclusions | 92 |
| 6. Real Measurement Under Virtual Topology..... | 95 |
| 6.1 Metrics | 96 |
| 6.2 Overloading Approach | 97 |
| 6.3 Measurement Procedure | 101 |
| 6.4 Results and Analysis | 105 |
| 6.5 Open Issues | 117 |
| 6.6 Conclusions | 121 |
| 7. Related Work | 123 |
| 7.1 General-Purpose Distribution Services | 123 |
| 7.2 Special-Purpose Distribution Services | 129 |
| 7.3 Information Delivery Structures | 132 |
| 7.4 Security | 134 |
| 7.5 Conclusions | 134 |
| 8. Future Work | 135 |
| 8.1 Open Issues Discussed in Previous Chapters | 135 |
| 8.2 Think More Beyond Today | 136 |
| 9. Conclusions | 139 |
| 9.1 Summary of the Problem | 139 |
| 9.2 The Revere Solution | 140 |
| 9.3 Contributions of Revere | 142 |
| 9.4 Broad Lessons | 143 |
| 9.5 Final Comments | 144 |
| References | 145 |
| Index | 153 |

List of Figures and Tables

Figures

| | | |
|------|--------------------------------------------------------------------|-----|
| 1.1 | IP addresses compromised by the “CodeRed” worm | 2 |
| 1.2 | Amount of patching in post-infection web servers | 3 |
| 3.1 | Application-layer overlay network on top of hardware layer | 25 |
| 3.2 | An RBone rooted at a dissemination center | 28 |
| 3.3 | Expanding-wheel topology | 32 |
| 3.4 | Three-way-handshake during join procedure | 33 |
| 3.5 | A new node’s three-way-handshake with four existing nodes | 35 |
| 3.6 | Path vector at node 5 | 36 |
| 3.7 | Parent selection based on path vector | 37 |
| 3.8 | Parent selection at node 5 | 38 |
| 3.9 | RBone messages | 41 |
| 3.10 | A common RBone based on a single rendezvous point | 44 |
| 3.11 | A common RBone based on multiple rendezvous points | 45 |
| 4.1 | The security update format | 50 |
| 4.2 | I/O jobs and security update window at a Revere node | 51 |
| 4.3 | Adaptive parent-to-child security update transmission | 52 |
| 4.4 | UDP-based pushing operation | 54 |
| 4.5 | TCP-based pushing operation | 55 |
| 4.6 | Bootstrap of dissemination jobs | 57 |
| 4.7 | Security update processing by an input job | 59 |
| 4.8 | Pulling security updates from repository servers | 61 |
| 5.1 | Integrity protection of a security update | 71 |
| 5.2 | The key invalidation message | 73 |
| 5.3 | Center public key invalidation | 74 |
| 5.4 | An input job function calling the security update protector | 79 |
| 5.5 | An output job function calling the security update protector | 79 |
| 5.6 | Peer-to-peer security scheme negotiation | 82 |
| 5.7 | Secured three-way-handshake procedure | 83 |
| 5.8 | Security box | 84 |
| 5.9 | Replay attack prevention using a random number | 89 |
| 6.1 | A virtual topology with 20 Revere nodes | 99 |
| 6.2 | Composition of security update dissemination latency | 103 |
| 6.3 | Prolonged dissemination latency in an overloaded environment . | 104 |
| 6.4 | Outbound bandwidth per node during joining phase | 107 |
| 6.5 | Join latency per node | 107 |
| 6.6 | Security update processing delay at a Revere node | 109 |
| 6.7 | Kernel-space-crossing latency | 109 |

| | | |
|------|-----------------------------------------------------------------------------------------|-----|
| 6.8 | Hop count of security update dissemination | 110 |
| 6.9 | Average and maximum security update dissemination latency ... | 112 |
| 6.10 | Security update dissemination coverage for a 3000-node dissemination | 113 |
| 6.11 | The latency to reach 99%, 90%, and 2/3 of nodes in an RBone .. | 114 |
| 6.12 | Resiliency test for a 3000-node dissemination with a 15% node failure | 116 |
| 6.13 | Resiliency test with different node broken probabilities on a 3000- node RBone | 117 |
| 6.14 | Monthly average Internet hosts in millions | 119 |

Tables

| | | |
|-----|---------------------------------------------|----|
| 3.1 | Main fields of a Joint data structure | 40 |
|-----|---------------------------------------------|----|

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.