

# Decompiling Java

GODFREY NOLAN

Apress®

**Decompiling Java**  
**Copyright © 2004 by Godfrey Nolan**

Lead Editor: Gary Cornell

Technical Reviewer: John Zukowski

Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, John Franklin, Jason Gilmore, Chris Mills, Steve Rycroft, Dominic Shakeshaft, Jim Sumser, Karen Watterson, Gavin Wray, John Zukowski

Project Manager: Tracy Brown Collins

Copy Edit Manager: Nicole LeClerc

Copy Editor: Rebecca Rider

Production Manager: Kari Brooks

Production Editor: Katie Stence

Proofreader: Linda Seifert

Compositor and Artist: Kinetic Publishing Services, LLC

Indexer: Rebecca Plunkett

Cover Designer: Kurt Krames

Manufacturing Manager: Tom Debolski

**Library of Congress Cataloging-in-Publication Data**

Nolan, Godfrey.

Decompiling Java / Godfrey Nolan.

p. cm.

Includes index.

ISBN 1-59059-265-4 (alk. paper)

1. Java (Computer program language) I. Title.

QA76.73.J38N65 2004

005.13'3—dc22

2004014051

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010 and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, e-mail [orders@springer-ny.com](mailto:orders@springer-ny.com), or visit <http://www.springer-ny.com>. Outside the United States: fax +49 6221 345229, e-mail [orders@springer.de](mailto:orders@springer.de), or visit <http://www.springer.de>.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail [info@apress.com](mailto:info@apress.com), or visit <http://www.apress.com>.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at <http://www.apress.com> in the Downloads section.

# Contents

About the Author .....	<i>ix</i>
About the Technical Reviewer .....	<i>xi</i>
Acknowledgments .....	<i>xiii</i>
 Chapter 1 Introduction .....	 <i>1</i>
Compilers and Decompilers .....	<i>2</i>
Virtual Machine Decompilers .....	<i>3</i>
Why Java? .....	<i>3</i>
History: Basic Chronology .....	<i>6</i>
Legal Issues .....	<i>9</i>
Moral Issues .....	<i>12</i>
Protecting Yourself .....	<i>13</i>
Book Outline .....	<i>15</i>
Conclusion .....	<i>16</i>
 Chapter 2 Ghost in the Machine .....	 <i>17</i>
The JVM: An Exploitable Design? .....	<i>18</i>
Inside a Classfile .....	<i>22</i>
Conclusion .....	<i>60</i>
 Chapter 3 Tools of the Trade .....	 <i>61</i>
Employing Hexadecimal Editors .....	<i>61</i>
The Problem of Insecure Code .....	<i>64</i>
Disassemblers .....	<i>67</i>
Decompilers .....	<i>72</i>
Obfuscators .....	<i>75</i>
Conclusion .....	<i>76</i>

<b>Chapter 4</b>	<b>Protecting Your Source: Strategies for Defeating Decompilers .....</b>	<b>79</b>
Compilation Flags .....		81
Writing Two Versions of the Applet or Application .....		86
Employing Obfuscation .....		88
Web Services and Server-Side Execution .....		106
Encryption .....		108
Digital Rights Management .....		109
Fingerprinting Your Code .....		110
Selling the Source Code .....		117
Native Methods .....		117
Conclusion .....		119
<b>Chapter 5</b>	<b>Decompiler Design .....</b>	<b>121</b>
Introduction .....		122
Defining the Problem .....		125
(De)Compiler Tools .....		128
Strategy .....		141
Parser Design .....		149
Conclusion .....		157
<b>Chapter 6</b>	<b>Decompiler Implementation .....</b>	<b>159</b>
ClassToXML Output: An Overview .....		159
JLex Specification .....		165
CUP Specification .....		170
Test Suite .....		182
Summarizing Decompiler Implementation .....		233
Conclusion .....		236
<b>Chapter 7</b>	<b>Case Studies .....</b>	<b>237</b>
Case Studies .....		237
Conclusion .....		244
<b>Appendix</b>	<b>Classfile Grammar .....</b>	<b>247</b>
<b>Index .....</b>		<b>255</b>