

Complements your Cisco Academy course instruction
in networking security!

Eric Cole

Network Security

Second Edition

Understand the changing
security landscape

Learn the latest approaches
and best practices

Secure your enterprise
and data worldwide



Bible

The book you need to succeed!

Network Security Bible

Network Security Bible

2nd Edition

**Eric Cole
Ronald Krutz
James W. Conley**



WILEY

Wiley Publishing, Inc.

Network Security Bible, 2nd Edition

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2009 by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-50249-5

Manufactured in the United States of America

10 9 8 7 6 5 4 3

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Control Number: 2009933372

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc. is not associated with any product or vendor mentioned in this book.

This book is dedicated to my father and to my family, who provided constant support and encouragement.

About the Author

Dr. Eric Cole is an industry-recognized security expert, technology visionary, and scientist. He is the author of many books, articles, and papers on cyber security and is one of the highest-rated speakers on the SANS training circuit. He has earned rave reviews for his ability to educate and train network security professionals worldwide. He has appeared on CNN and has been interviewed on various TV programs, including *CBS News* and *60 Minutes*.

Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. He has experience in information technology, with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. An information security expert for more than 20 years, he holds several professional certificates and helped develop several certifications and corresponding courses. He obtained his M.S. in computer science at the New York Institute of Technology and earned his doctorate in network security from Pace University.

Dr. Cole has created and directed corporate security programs for several large organizations, built numerous security consulting practices, and worked for more than five years at the Central Intelligence Agency. He is currently chief scientist and senior fellow for Lockheed Martin. He also was a member of the Commission on Cyber Security during the administration of President George W. Bush, and has been actively involved with many sectors of cyber security including government, energy, nuclear, financial, and pharmaceutical.

About the Technical Editor

Dr. Ronald L. Krutz is a senior information system security consultant. Earlier, he was chief technical officer for Threatscape Solutions, Inc., and a senior information systems security researcher in the Advanced Technology Research Center of Lockheed Martin Information Technologies. He has more than 30 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training.

Credits

Executive Editor
Carol Long

Project Editor
William Bridges

Technical Editor
Ronald Krutz

Production Editor
Rebecca Anderson

Copy Editor
Nancy Rapoport

Editorial Director
Robyn B. Siesky

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

**Vice President and Executive Group
Publisher**
Richard Swadley

Vice President and Executive Publisher
Barry Pruett

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Lynsey Stanford

Proofreader
Jen Larsen, Word One

Indexer
J & J Indexing

Cover Image
Joyce Haughey

Cover Designer
Michael E. Trent

Acknowledgments

Wiley is a wonderful publishing company to work with. Carol Long is an insightful and energetic executive editor who provides continual support. William Bridges provided constant guidance and expertise, and without all his help and hard work this book would not be where it is today.

As deadlines approach you reach out to your co-workers who are truly friends to tap into their expertise and knowledge. AJ Jackson, Tom Prunier, and Ronnie Fabela all helped with the book.

This book would not have been completed without the author's opportunity to work for such a great company, Lockheed Martin. Continuing thanks to Linda Gooden, Richard Johnson, Charlie Croom and Lee Holcomb for allowing creative minds to think of solutions to complex technical problems. Lockheed Martin's support is critical to the success of this book and the success of the cutting-edge results the team produces.

Most of all I want to thank God for blessing me with a great life and a wonderful family.

I have Kerry, who is a loving and supportive wife. Without her none of this would be possible. My wonderful son, Jackson, and my princesses, Anna and Abby, bring joy and happiness to me every day.

While he was taken from us too soon, my father has always been my biggest fan and supporter. We would always want more time with those we love. Ron Cole was the best father anyone could ever ask. He taught me to never give up and always to exceed expectations. His guidance, direction, and insight will live with me forever.

In addition, thanks to all friends, family, and co-workers who have been a support in a variety of ways through this entire process.



Introduction	xxxv
Part I: Network Security Landscape	
Chapter 1: State of Network Security	3
Chapter 2: New Approaches to Cyber Security	9
Chapter 3: Interfacing with the Organization	19
Part II: Security Principles and Practices	
Chapter 4: Information System Security Principles	35
Chapter 5: Information System Security Management	73
Chapter 6: Access Control	109
Chapter 7: Attacks and Threats	127
Part III: Operating Systems and Applications	
Chapter 8: Windows Security	145
Chapter 9: UNIX and Linux Security	207
Chapter 10: Web Browser and Client Security	255
Chapter 11: Web Security	287
Chapter 12: Electronic mail (E-mail) Security	323
Chapter 13: Domain Name System	357
Chapter 14: Server Security	395
Part IV: Network Security Fundamentals	
Chapter 15: Network Protocols	431
Chapter 16: Wireless Security	459
Chapter 17: Network Architecture Fundamentals	509
Chapter 18: Firewalls	531
Chapter 19: Intrusion Detection/Prevention	549
Part V: Communication	
Chapter 20: Secret Communication	571
Chapter 21: Covert Communication	631
Chapter 22: Applications of Secure/Covert Communication	681
Part VI: The Security Threat and Response	
Chapter 23: Intrusion Detection and Response	707
Chapter 24: Digital Forensics	729
Chapter 25: Security Assessments, Testing, and Evaluation	751

Contents at a Glance

Part VII: Integrated Cyber Security

Chapter 26: Validating Your Security	777
Chapter 27: Data Protection	797
Chapter 28: Putting Everything Together	809
Chapter 29: The Future	835
Index	849

The primary security issue related to JavaScript is that when viewed on a Web site it has the ability to open new browser windows without your permission. Just by adding the following lines to an HTML file, the Web site `www.google.com` will open in a separate window without any interaction by the user.

```
<SCRIPT>
window.open("http://www.google.com", '' + 0 + '', 'toolbar=0,
scrollbars=1,location=0,statusbar=0,menubar=0,resizable=0,
width=1152,height=864');
</SCRIPT>
```

This is one of the ways that Web sites create pop-up advertisements. While those ads can be annoying, they are generally not security threats. The danger comes when the opened Web site is operated by a malicious user. These types of attacks have been known to be capable of stealing passwords, PINs, credit card numbers, cause the computer to crash, and monitor all activity performed by the browser.

Although all current (known) vulnerabilities have been patched, JavaScript has the potential to access anything that the browser can if a new vulnerability is discovered. As with any client-side executable, JavaScript should be disabled if high security is a concern and sensitive information is present on the host computer.

Java

Java is a language created by Sun Microsystems in 1991 to provide a method to execute programs without any platform dependence. Although originally intended for small consumer electronic devices such as VCRs, toasters, and television sets, its popularity soared in 1994 when it was used across the Internet.

The sandbox and security

The Java security model is based on the notion of a sandbox. This environment resides on the host computer that is executing the Java application, and is designed to confine the program to a small play area. This play area is the sandbox, and it contains no critical resources. All access is explicitly granted by the user.

By default, the application only has access to the central processing unit (CPU), the display, the keyboard, the mouse, and its own memory. This provides the program with what it needs to run, but does not afford it what it needs to be dangerous.

Trusted applications can be provided larger boundaries and access to additional information. For example, applications that share files or documents may require additional access to the hard drive.

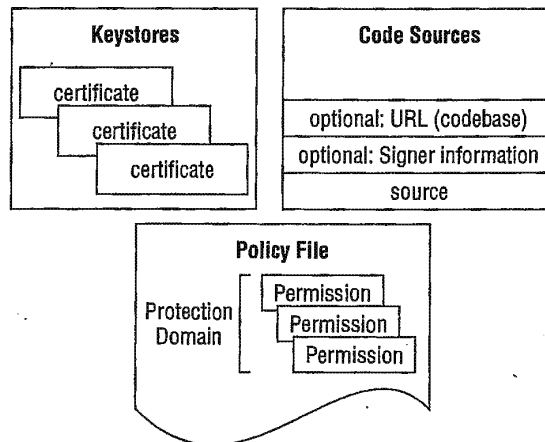
The Java sandbox is composed of the following:

- **Permissions** — Explicit statements of actions that applications are allowed to execute and resources that they are allowed to access.
- **Protection domains** — Collections of permissions that describe what actions applications from domains are allowed to execute and resources that they can access.
- **Policy files** — Contains protection domains.
- **Code stores** — The sites that the applications are physically stored on prior to execution on the host.
- **Certificates** — Used to sign code to convey trust to a user that you are the developer of the application.
- **Key stores** — Files that contain the certificates for Web sites. Key stores are queried to identify who signed the application code.

Figure 11-7 depicts the Java security model.

FIGURE 11-7

The Java security model involves the policy file, protection domain, code sources, key stores, and certificates.



Types of Java permissions

Table 11-2 shows the different permissions that are allowed in Java and what the resulting actions are.

TABLE 11-2

Java Permissions Summary

Type	Name	Actions
java.io. FilePermission	File to perform action on	Read, write, delete, execute
java.net. SocketPermission	hostname:port	Accept, listen, connect, resolve
java.util. PropertyPermission	Java virtual machine that you want to perform action on	Read, write
java.lang. RuntimePermission	Specific to the class, examples within the core Java API include the following: <i>createClassLoader</i> , <i>readFileDescriptor</i> , <i>exitVM</i> , and <i>setIO</i>	Actions are not used; you either have permission to execute the specific runtime operation or you do not
Java.awt. AWTPermissions	<i>accessClipboard</i> , <i>accessEventQueue</i> , <i>createRobot</i> , <i>listenToAllAWTEvents</i> , <i>readDisplayPixels</i> , and <i>showWindowWithoutWarningBanner</i>	Not used
Java.net. NetPermission	<i>specifyStreamHandler</i> , <i>setDefaultAuthenticator</i> , <i>requestPasswordAuthentication</i>	Not used
Java.security. SecurityPermission	There are several; popular examples include the following: <i>addIdentityCertificate</i> , <i>getPolicy</i> , <i>setPolicy</i> , <i>setSystemScope</i>	Not used
Java.io. SerializablePermission	<i>enableSubstitution</i> , <i>enableSubclassImplementation</i>	Not used
Java.lang.reflect. ReflectPermission	<i>suppressAccessChecks</i>	Not used
Java.security. AllPermission	None	Not used

ActiveX

ActiveX is one of the most powerful technologies available today. Using it, software can be automatically downloaded, installed, and executed. ActiveX can be thought of as a self-installing plug-in. If configured by the browser, Web pages that contain an OBJECT tag are automatically acted upon simply by viewing.

passwords when they forget them. In such cases, the system administrator must enter a new password for the user, which the user can change upon re-entering the application.

- Credit card and other financial information should never be sent in the clear.
- Servers should minimize the transmissions and printing of credit card information. This includes all reports that may be used for internal use, such as troubleshooting, status, and progress reports.
- Sensitive data should not be passed to the server as part of the query string, such as in the following. The query string may be recorded in logs and accessed by persons not authorized to see the credit card information. For example:

```
http://www.server-site.com/process_card.asp?cardnumber=1234567890123456
```

Keeping code clean

When it comes to information put into server code, a good motto might be, "Be paranoid. Don't disclose any more than necessary." Attackers will spend countless hours gathering information looking for the nugget that will make their task easier. Much of that time will be spent examining HTML and scripts for information that can be used to make their attack easier.

Comments should be stripped from operational code. Names and other personal information, in particular, should be avoided. HTML comment fields should not reveal exploitable information about the developers or the organization. Comments are not bad per se, but those embedded in the HTML or client script and which may contain private information can be very dangerous in the hands of an attacker.

Many times third-party software packages, such as Web servers and FTP servers, will provide banners that indicate the version of the software that is running. Attackers can use this information to narrow their search of exploits to apply to these targets. In most cases, these banners can be suppressed or altered.

Choosing the language

One of the most frequently discovered vulnerabilities in server applications is a direct result of the use of C and C++. The C language is unable to detect and prevent improper memory allocation, which can result in a buffer overflow.

Because the C language cannot prevent buffer overflows, it is left to the programmer to implement safe programming techniques. Good coding practices will check for boundary limits and make sure that the function was properly called. This requires a great deal of discipline from the programmer and, in practice, even the most experienced developers can overlook these checks occasionally.

One of the reasons Java is so popular is because of its intrinsic security mechanisms. Malicious language constructs should not be possible in Java. The Java Virtual Machine (JVM) is responsible for stopping buffer overflows, the use of un-initialized variables, and the use of invalid opcodes.

If you're in charge of network security, you need this book

Since the first edition of this comprehensive guide, cyber threats have increased, the stakes have gotten higher, and what is considered state of the art security has evolved. This packed new edition, thoroughly revised to cover the very latest techniques, is the detailed wall-to-wall resource you need to keep your network secure. Understand the changing threats, find out what *defense in depth* means and why you need it, learn best practices, and take control with this must-have book.

- Understand current threats and attacks and how they succeed
- Answer 30 critical questions and see how your network security is today
- Consider mission resilience and make sure your critical functions survive
- Master crypto, steganography, VPN, and other covert communications
- Learn effective techniques for Windows®, Linux®, browser, e-mail, and wireless security
- Explore the basics of digital forensics, including evidence preservation
- Do risk analysis, make a global plan, and prepare for business continuity and recovery

Eric Cole

holds a PhD and CISSP and has been a security consultant for international banks and the Fortune 500. He made his mark working for the CIA for more than seven years and as a member of the HoneyNet Project. He was also a member of the Commission on Cyber Security for the 44th Presidency. He has appeared as a security expert on *CBS News* and *60 Minutes* and is a regular security expert for *CNN Headline News*.



Shelving Category:
COMPUTERS / Security

Reader Level:
Beginning to Advanced

\$59.99 USA
\$71.99 Canada

ISBN 978-0-470-50249-5

