"**Practical Intrusion Analysis** *provides a solid fundamental overview of the art and science of intrusion analysis.*"
—**Nate Miller,** Cofounder, Stratum Security

PRACTICAL INTRUSION ANALYSIS

Prevention and Detection for the Twenty-First Century

RYAN TROST

Practical Intrusion Analysis

This page intentionally left blank

Practical Intrusion Analysis

Prevention and Detection for the Twenty-First Century

Ryan Trost

Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Library of Congress Cataloging-in-Publication Data:

Trost, Ryan.

Practical intrusion analysis : prevention and detection for the twenty-first century / Ryan Trost.

p. cm.

Includes index.

ISBN-13: 978-0-321-59180-7 (pbk. : alk. paper)

ISBN-10: 0-321-59180-1

1. Computer networks--Security measures. 2. Computer networks--Monitoring. 3. Computer security. 4. Computers--Access control. I. Title.

TK5105.59.T76 2009

005.8--dc22

2009019158

ISBN-13: 978-0-321-59180-7
ISBN-10: 0-321-59180-1

Text printed in the United States on recycled paper at R.R. Donnelley in Crawfordsville, Indiana.

First printing July 2009

Editor-in-Chief
Karen Gettman

Acquisitions Editor
Jessica Goldstein

Senior Development Editor
Chris Zahn

Managing Editor
Kristy Hart

Project Editor
Jovana San Nicolas-Shirley

Copy Editor
Sheri Cain

Indexer
Erika Millen

Proofreader
Debbie Williams

Publishing Coordinator
Romny French

Cover Designer
Chuti Prasertsith

Compositor
Jake McFarland

To my loving wife, Kasey, who is pregnant with our first beautiful child.

To my supportive families: To my parents, sister, and brother, who have supported me, motivated me and somehow sustained my endless IT ramblings. And to my wife's family, the Arbacas clan, who have only had to endure my InfoSec rambling for a couple years and still invite me to dinner. I very much appreciate all the help and support!

This page intentionally left blank

Contents