silence on the wire

a Field Guide to Passive Reconnaissance and Indirect Attacks

Michal Zalewski

SILENCE ON THE WIRE

SILENCE ON THE WIRE

A Field Guide to Passive Reconnaissance and Indirect Attacks

by Michal Zalewski

no starch press

San Francisco

15 14 13 12 6 7 8 9

ISBN-10: 1-59327-046-1
ISBN-13: 978-1-59327-046-9

Publisher: William Pollock
Managing Editor: Karol Jurado
Production Manager: Susan Berge
Cover and Interior Design: Octopod Studios
Developmental Editors: William Pollock and John Mark Walker
Technical Reviewer: Solar Designer
Copyeditor: Pat Coleman
Compositor: Riley Hoffman
Proofreader: Stephanie Provines
Indexer: Ted Laux

For information on book distributors or translations, please contact No Starch Press, Inc. directly:

No Starch Press, Inc.
555 De Haro Street, Suite 250, San Francisco, CA 94107
phone: 415.863.9900; fax: 415.863.9950; info@nostarch.com; http://www.nostarch.com

Library of Congress Cataloging-in-Publication Data

```
Zalewski, Michal.
  Silence on the wire : a field guide to passive reconnaissance and indirect attacks / Michal
Zalewski.
       p. cm.
  Includes index.
  ISBN 1-59327-046-1
1.  Computer networks--Security measures.  I. Title.
   TK5105.59.Z35 2005
   005.8--dc22
                                                    2004009744
```

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

For Maja

ABOUT THE AUTHOR

Michal Zalewski is a self-taught information security researcher who has worked on topics ranging from hardware and OS design principles to networking. He has been a prolific bug hunter and a frequent Bugtraq poster since the mid ’90s and has authored popular security utilities such as p0f, a passive OS fingerprinter. He has also published a number of acclaimed security research papers. Michal has worked as a security expert for several reputable companies, both in his native Poland and the U.S., including two major telecoms. In addition to being an avid researcher and occasional coder, Michal dabbles in the fields of artificial intelligence, applied mathematics, and electronics, and is also an amateur photographer.

BRIEF CONTENTS

CONTENTS IN DETAIL

PART II: SAFE HARBOR

On the threats that lurk in between the computer and the Internet

FOREWORD

What does it take to write a novel book on computer security? Or rather, what does it take to write a novel on modern computing?

A young yet highly experienced author with talents in many areas including many aspects of computing, mathematics, and electronics (and perhaps a hobby in robotics), as well as other seemingly unrelated interests (including, let's say, fatalistic erotic photography), and indeed with a talent and desire to write.

> *Once upon a time in a dark and largely unexplored forest, the magic chemistry of (brain cell) trees gave birth to a bit of information, only to let him sail his way down a quick river, into the vast sea (of the Internet), and ultimately find his new home, grave, or maybe a place in a museum.*
>
> *And so the tale begins. Whether our little bit is good or evil, at a young age he will reach the stream flowing into a shiny castle made out of white-colored foil (yet regarded by many as a black box). He will pass through the entrance and approach the counter to check in. If he weren't so naive and short-sighted, he could notice a group of evil-looking bits staring at the counter from a distance, taking note of the time bits check in and out; he would have no choice but to proceed to sign in, though.*

Once rested, our hero might be asked to team up with his siblings or to join a group of other bits and bitesses, and together they would pack their bodies tightly onto a used inflatable boat. A careful bit could notice bits of garbage (or is that garbage?) in the boat, presumably left by a previous group.

Observing the traffic lights and squeezing through traffic jams, our bits enter a safe harbor and sail to the wharf. Will they be seen from nearby castles and lighthouses? Will someone track the traffic light switches to determine just when our group sailed? Will someone turn on lights at the wharf and take pictures? Will those other evil bits assume the identity of ours and sail away to the sea first? Our bits wouldn't know.

And so they change boats at the wharf and sail to the sea . . . The journey of our pet bits proceeds, with many dangers yet to come.

No, Michal's book does not hide technical detail behind a fairy tale as I have above. Rather, while a very entertaining read, it gets all the facts straight and promptly gives answers to most challenges introduced at the beginning of each chapter.

Silence on the Wire is unique in many aspects, but two stand out: First, it provides in-depth coverage of almost all essential stages of data processing that enable today's "internetworking"—from a keypress to the intended end result of that keypress. Second, it outlines the largely overlooked, under-researched, and inherent security issues associated with each stage of networking and with the process as a whole. The security issues covered serve well to demonstrate the art of vulnerability research from both the attacker's and the defender's perspective, and will encourage further research on the part of the reader.

Clearly, a computer security book can't be comprehensive. In *SotW*, Michal has provocatively chosen to leave out all the well known yet highly dangerous and widespread vulnerabilities and attacks being discussed and worked on today by most in the information security community. He will teach you about subtle keystroke timing attacks, but you will not be reminded that "trojan horse" software with key logging capabilities is currently both more common and easier to use than any of such attacks could ever be.

Why mention keystroke timings while leaving the trojans out? Because timing attacks are largely underappreciated and misunderstood even by information security professionals, whereas trojans are a widely known and obvious threat. Vulnerability to timing attacks is a property of the design of many components involved, whereas to implant a trojan requires either a software bug or an end-user error.

Similarly, and with few exceptions, you won't find the slightest mention in *SotW* of the widely exploited software bugs—or even generic software bug classes such as "buffer overflows." If you are not already familiar with the

common computer security threats and would like to gain that knowledge, you will need to accompany yourself on your journey through this book with the perusal of less exciting material available on the Internet and in other books, and in particular with material pertaining to the specific operating systems that you use.

Why study silence, you may wonder—isn't that a nothing? Yes, in a sense. A zero is a nothing in that sense, too. But it is also a number, a concept we cannot really understand the world without.

Enjoy the silence—the best you can.

Alexander Peslyak
Founder and CTO
Openwall, Inc.

better known as

Solar Designer
Openwall Project leader

January 2005

INTRODUCTION

A Few Words about Me

I seem to have been born a computer geek, but my adventure with network security began only by accident. I have always loved to experiment, explore new ideas, and solve seemingly well defined but still elusive challenges that require innovative and creative approaches—even if just to fail at solving them. When I was young, I spent most of my time pursuing sometimes risky and often silly attempts to explore the world of chemistry, mathematics, electronics, and finally computing rather than ride my bike around the block all day long. (I probably exaggerate a bit, but my mother always seemed to be worried.)

Shortly after my first encounter with the Internet (in the mid '90s, perhaps eight years after I coded my first "Hello world" program on a beloved 8-bit machine), I received an unusual request: a spam letter that, hard to believe, asked me (and a couple thousand other folks) to join an underground team of presumably malicious, black hat hackers. This did not drive me underground (perhaps due to my strong instinct for self-preservation, known in certain circles as cowardice) but somehow provided a good motivation to explore the field of computer security in more detail. Having done plenty of amateur programming, I found it captivating to look at code from a different perspective and to try to find a way for an algorithm to do something more than it was supposed to do. The Internet seemed a