



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

SILENCE ON THE WIRE. Copyright © 2005 by Michal Zalewski.

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.

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.

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. 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 it.

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

Foreword

xix

Introduction

xxiii

Part I: The Source

Chapter 1

I Can Hear You Typing

3

Chapter 2

Extra Efforts Never Go
Unnoticed

21

Chapter 3

Ten Heads of the Hydra

51

Chapter 4

Working for
the Common Good

57

Part II: Safe Harbor

Chapter 5

Blinkenlights

65

Chapter 6

Echoes of the Past

89

Chapter 7

Secure in Switched Networks

95

Chapter 8

Us versus Them

103

Part III: Out in the Wild

Chapter 9

Foreign Accent
113

Chapter 10

Advanced
Sheep-Counting Strategies
151

Chapter 11

In Recognition of Anomalies
173

Chapter 12

Stack Data Leaks
189

Chapter 13

Smoke and Mirrors
193

Chapter 14

Client Identification:
Papers, Please!
199

Chapter 15

The Benefits of Being a Victim
219

Part IV: The Big Picture

Chapter 16

Parasitic Computing,
or How Pennies Add Up
227

Chapter 17

Topology of the Network
243

Chapter 18

Watching the Void
253

Closing Words

261

Bibliographic Notes

263

Index

269

CONTENTS IN DETAIL

FOREWORD <i>by Solar Designer</i>	xix
---	------------

INTRODUCTION	xxiii
A Few Words about Me	xxiii
About This Book	xxiv

PART I: THE SOURCE

On the problems that surface long before one sends any information over the network

1 I CAN HEAR YOU TYPING	3
<i>Where we investigate how your keystrokes can be monitored from far, far away</i>	

The Need for Randomness	4
Automated Random Number Generation	6
The Security of Random Number Generators	7
I/O Entropy: This Is Your Mouse Speaking	8
Delivering Interrupts: A Practical Example	8
One-Way Shortcut Functions	11
The Importance of Being Pedantic	12
Entropy Is a Terrible Thing to Waste	13
Attack: The Implications of a Sudden Paradigm Shift	14
A Closer Look at Input Timing Patterns	15
Immediate Defense Tactics	18
Hardware RNG: A Better Solution?	18
Food for Thought	19
Remote Timing Attacks	19
Exploiting System Diagnostics	20
Reproducible Unpredictability	20

2 EXTRA EFFORTS NEVER GO UNNOTICED	21
<i>Where we learn how to build a wooden computer and how to obtain information from watching a real computer run</i>	

Boole's Heritage	21
Toward the Universal Operator	22
DeMorgan at Work	23

Convenience Is a Necessity	24
Embracing the Complexity	25
Toward the Material World	25
A Nonelectric Computer	26
A Marginally More Popular Computer Design	27
Logic Gates	27
From Logic Operators to Calculations	28
From Electronic Egg Timer to Computer	31
Turing and Instruction Set Complexity	32
Functionality, at Last	34
Holy Grail: The Programmable Computer	35
Advancement through Simplicity	35
Split the Task	36
Execution Stages	37
The Lesser Memory	38
Do More at Once: Pipelining	39
The Big Problem with Pipelines	40
Implications: Subtle Differences	41
Using Timing Patterns to Reconstruct Data	42
Bit by Bit	42
In Practice	44
Early-Out Optimization	44
Working Code—Do It Yourself	46
Prevention	48
Food for Thought	49

3 **TEN HEADS OF THE HYDRA** **51**

Where we explore several other tempting scenarios that occur very early on in the process of communications

Revealing Emissions: TEMPEST in the TV	52
Privacy, Limited	53
Tracking the Source: "He Did It!"	54
"Oops" Exposure: *_~1q!@@ . . . and the Password Is	55

4 **WORKING FOR THE COMMON GOOD** **57**

Where a question of how the computer may determine the intent of its user is raised and left unanswered

PART II: SAFE HARBOR

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

5 BLINKENLIGHTS 65

Where we conclude that pretty can also be deadly, and we learn to read from LEDs

The Art of Transmitting Data	66
From Your Email to Loud Noises . . . Back and Forth	68
The Day Today	73
Sometimes, a Modem Is Just a Modem	74
Collisions Under Control	75
Behind the Scenes: Wiring Soup and How We Dealt with It	76
Blinkenlights in Communications	78
The Implications of Aesthetics	80
Building Your Own Spy Gear . . .	81
. . . And Using It with a Computer	82
Preventing Blinkenlights Data Disclosure—and Why It Will Fail	85
Food for Thought	88

6 ECHOES OF THE PAST 89

Where, on the example of a curious Ethernet flaw, we learn that it is good to speak precisely

Building the Tower of Babel	90
The OSI Model	91
The Missing Sentence	92
Food for Thought	94

7 SECURE IN SWITCHED NETWORKS 95

Or, why Ethernet LANs cannot be quite fixed, no matter how hard we try

Some Theory	96
Address Resolution and Switching	96
Virtual Networks and Traffic Management	97
Attacking the Architecture	99
CAM and Traffic Interception	100
Other Attack Scenarios: DTP, STP, Trunks	100
Prevention of Attacks	101
Food for Thought	101

8
US VERSUS THEM **103**

What else can happen in the local perimeter of “our” network? Quite a bit!

Logical Blinkenlights and Their Unusual Application	105
Show Me Your Typing, and I Will Tell You Who You Are	105
The Unexpected Bits: Personal Data All Around	106
WiFi Vulnerabilities	107

PART III: OUT IN THE WILD

Once you are on the Internet, it gets dirty

9
FOREIGN ACCENT **113**

Passive fingerprinting: subtle differences in how we behave can help others tell who we are

The Language of the Internet	114
Naive Routing	115
Routing in the Real World	116
The Address Space	116
Fingerprints on the Envelope	118
Internet Protocol	118
Protocol Version	119
The Header Length Field	119
The Type of Service Field (Eight Bits)	120
The Total Packet Length (16 Bits)	120
The Source Address	120
The Destination Address	121
The Fourth Layer Protocol Identifier	121
Time to Live (TTL)	121
Flags and Offset Parameters	122
Identification Number	123
Checksum	124
Beyond Internet Protocol	124
User Datagram Protocol	125
Introduction to Port Addressing	125
UDP Header Summary	126
Transmission Control Protocol Packets	126
Control Flags: The TCP Handshake	127
Other TCP Header Parameters	130
TCP Options	132
Internet Control Message Protocol Packets	134
Enter Passive Fingerprinting	135
Examining IP Packets: The Early Days	135
Initial Time to Live (IP Layer)	136
The Don't Fragment Flag (IP Layer)	136
The IP ID Number (IP Layer)	137

Type of Service (IP Layer)	137
Nonzero Unused and Must Be Zero Fields (IP and TCP Layers)	138
Source Port (TCP Layer)	138
Window Size (TCP Layer)	139
Urgent Pointer and Acknowledgment Number Values (TCP Layer)	139
Options Order and Settings (TCP Layer)	140
Window Scale (TCP Layer, Option)	140
Maximum Segment Size (TCP Layer, Option)	140
Time-Stamp Data (TCP Layer, Option)	140
Other Passive Fingerprinting Venues	141
Passive Fingerprinting in Practice	142
Exploring Passive-Fingerprinting Applications	143
Collecting Statistical Data and Incident Logging	144
Content Optimization	144
Policy Enforcement	144
Poor Man's Security	145
Security Testing and Preattack Assessment	145
Customer Profiling and Privacy Invasion	145
Espionage and Covert Reconnaissance	146
Prevention of Fingerprinting	146
Food for Thought: The Fatal Flaw of IP Fragmentation	147
Breaking TCP into Fragments	148

10
ADVANCED SHEEP-COUNTING STRATEGIES **151**

Where we dissect the ancient art of determining network architecture and computer's whereabouts

Benefits and Liabilities of Traditional Passive Fingerprinting	151
A Brief History of Sequence Numbers	154
Getting More Out of Sequence Numbers	155
Delayed Coordinates: Taking Pictures of Time Sequences	156
Pretty Pictures: TCP/IP Stack Gallery	160
Attacking with Attractors	166
Back to System Fingerprinting	169
ISNProber—Theory in Action	169
Preventing Passive Analysis	170
Food for Thought	171

11
IN RECOGNITION OF ANOMALIES **173**

Or what can be learned from subtle imperfections of network traffic

Packet Firewall Basics	174
Stateless Filtering and Fragmentation	175
Stateless Filtering and Out-of-Sync Traffic	176
Stateful Packet Filters	177
Packet Rewriting and NAT	178
Lost in Translation	179

The Consequences of Masquerading	180
Segment Size Roulette	181
Stateful Tracking and Unexpected Responses	183
Reliability or Performance: The DF Bit Controversy	184
Path MTU Discovery Failure Scenarios	184
The Fight against PMTUD, and Its Fallout	186
Food for Thought	186

12
STACK DATA LEAKS **189**

Yet another short story on where to find what we did not intend to send out at all

Kristijan's Server	189
Surprising Findings	190
Revelation: Phenomenon Reproduced	191
Food for Thought	192

13
SMOKE AND MIRRORS **193**

Or how to disappear with grace

Abusing IP: Advanced Port Scanning	194
Tree in the Forest: Hiding Yourself	194
Idle Scanning	195
Defense against Idle Scanning	197
Food for Thought	198

14
CLIENT IDENTIFICATION: PAPERS, PLEASE! **199**

Seeing through a thin disguise may come in handy on many occasions

Camouflage	200
Approaching the Problem	201
Towards a Solution	201
A (Very) Brief History of the Web	202
A HyperText Transfer Protocol Primer	203
Making HTTP Better	205
Latency Reduction: A Nasty Kludge	205
Content Caching	207
Managing Sessions: Cookies	209
When Cookies and Caches Mix	210
Preventing the Cache Cookie Attack	211
Uncovering Treasons	211
A Trivial Case of Behavioral Analysis	212
Giving Pretty Pictures Meaning	214
Beyond the Engine	215
. . . And Beyond Identification	216

Prevention	217
Food for Thought	217

15
THE BENEFITS OF BEING A VICTIM **219**

In which we conclude that approaching life with due optimism may help us track down the attacker

Defining Attacker Metrics	220
Protecting Yourself: Observing Observations	223
Food for Thought	224

PART IV: THE BIG PICTURE

Our legal department advised us not to say “the network is the computer” here

16
PARASITIC COMPUTING, OR HOW PENNIES ADD UP **227**

Where the old truth that having an army of minions is better than doing the job yourself is once again confirmed

Nibbling at the CPU	228
Practical Considerations	231
Parasitic Storage: The Early Days	232
Making Parasitic Storage Feasible	234
Applications, Social Considerations, and Defense	241
Food for Thought	242

17
TOPOLOGY OF THE NETWORK **243**

On how the knowledge of the world around us may help track down friends and foes

Capturing the Moment	244
Using Topology Data for Origin Identification	245
Network Triangulation with Mesh-Type Topology Data	248
Network Stress Analysis	248
Food for Thought	251

18
WATCHING THE VOID **253**

When looking down the abyss, what does not kill us makes us stronger

Direct Observation Tactics	254
Attack Fallout Traffic Analysis	256

Detecting Malformed or Misdirected Data	259
Food for Thought	260

CLOSING WORDS	261
<i>Where the book is about to conclude</i>	

BIBLIOGRAPHIC NOTES	263
----------------------------	------------

INDEX	269
--------------	------------

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 naïve 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

sample content of Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks

- [download Queen Sugar](#)
- [Liberty Abroad: J. S. Mill on International Relations \(Ideas in Context\) here](#)
- [download Grenze im Nichts \(Perry Rhodan SilberbÄnde, Band 108; Die Kosmischen Burgen, Band 3\)](#)
- **[download online The Corporate Whistleblower's Survival Guide: A Handbook for Committing the Truth book](#)**
- [download online Militant Modernism](#)

- <http://junkrobots.com/ebooks/SAS-Survival-Handbook--The-Ultimate-Guide-to-Surviving-Anywhere--3rd-Edition-.pdf>
- <http://xn--d1aboelcb1f.xn--p1ai/lib/Michael-Freeman-s-101-Top-Digital-Photography-Tips.pdf>
- <http://transtrade.cz/?ebooks/Real-Marriage--The-Truth-About-Sex--Friendship--and-Life-Together.pdf>
- <http://junkrobots.com/ebooks/The-Stargate-Conspiracy--The-Truth-about-Extraterrestrial-life-and-the-Mysteries-of-Ancient-Egypt.pdf>
- <http://berttrotman.com/library/Militant-Modernism.pdf>