



The Myths of Security

What the Computer Security Industry
Doesn't Want You to Know

John Viega

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

Contents

Foreword	ix
Preface	xiii
Chapter 1	
The Security Industry Is Broken	1
Chapter 2	
Security: Nobody Cares!	5
Chapter 3	
It's Easier to Get "Owned" Than You Think	9
Chapter 4	
It's Good to Be Bad	19
Chapter 5	
Test of a Good Security Product: Would I Use It?	25
Chapter 6	
Why Microsoft's Free AV Won't Matter	29
Chapter 7	
Google Is Evil	33
Chapter 8	
Why Most AV Doesn't Work (Well)	41
Chapter 9	
Why AV Is Often Slow	49
Chapter 10	
Four Minutes to Infection?	55
Chapter 11	
Personal Firewall Problems	59
Chapter 12	
Call It "Antivirus"	65
Chapter 13	
Why Most People Shouldn't Run Intrusion Prevention Systems	71
Chapter 14	
Problems with Host Intrusion Prevention	75

Chapter 15	
Plenty of Phish in the Sea	79
Chapter 16	
The Cult of Schneier	87
Chapter 17	
Helping Others Stay Safe on the Internet	91
Chapter 18	
Snake Oil: Legitimate Vendors Sell It, Too	95
Chapter 19	
Living in Fear?	99
Chapter 20	
Is Apple Really More Secure?	105
Chapter 21	
OK, Your Mobile Phone Is Insecure; Should You Care?	109
Chapter 22	
Do AV Vendors Write Their Own Viruses?	113
Chapter 23	
One Simple Fix for the AV Industry	115
Chapter 24	
Open Source Security: A Red Herring	119
Chapter 25	
Why SiteAdvisor Was Such a Good Idea	127
Chapter 26	
Is There Anything We Can Do About Identity Theft? .	129
Chapter 27	
Virtualization: Host Security's Silver Bullet?	135
Chapter 28	
When Will We Get Rid of All the Security Vulnerabilities?	139
Chapter 29	
Application Security on a Budget	145
Chapter 30	
"Responsible Disclosure" Isn't Responsible	153
Chapter 31	
Are Man-in-the-Middle Attacks a Myth?	163
Chapter 32	
An Attack on PKI	167

Chapter 33	
HTTPS Sucks; Let's Kill It!	171
Chapter 34	
CrAP-TCHA and the Usability/Security Tradeoff	175
Chapter 35	
No Death for the Password	181
Chapter 36	
Spam Is Dead	187
Chapter 37	
Improving Authentication	191
Chapter 38	
Cloud Insecurity?	197
Chapter 39	
What AV Companies Should Be Doing (AV 2.0)	203
Chapter 40	
VPNs Usually Decrease Security	213
Chapter 41	
Usability and Security	215
Chapter 42	
Privacy	217
Chapter 43	
Anonymity	219
Chapter 44	
Improving Patch Management	221
Chapter 45	
An Open Security Industry	223
Chapter 46	
Academics	225
Chapter 47	
Locksmithing	227
Chapter 48	
Critical Infrastructure	229
Epilogue	231
Index	233