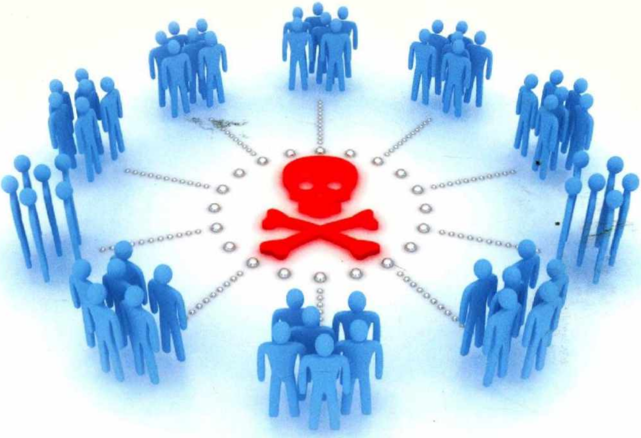
THE DEATH OF THE INTERNET



Edited by

MARKUS JAKOBSSON

WILEY

高等教育出版社
HIGHER EDUCATION PRESS

IEEE

IEEE computer society

The Death of the Internet

Edited by

Markus Jakobsson

IEEE
IEEE PRESS

IEEE computer society

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION

高等教育出版社
HIGHER EDUCATION PRESS

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 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 formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Jakobsson, Markus.
The death of the Internet / by Markus Jakobsson.
pages cm
Includes bibliographical references.
ISBN 978-1-118-06241-8 (pbk.)
1. Internet–Security measures. 2. Electronic commerce–Security measures.
3. Data protection. 4. Computer crimes. I. Title.
TK5105.875.I57J34 2012
005.8–dc23

2011047198

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For A and Art.

Contents

Foreword **xv**

Preface **xvii**

Is the Title of this Book a Joke? **xix**

Acknowledgments **xxi**

Contributors **xxiii**

Part I The Problem

1 What Could Kill the Internet? And so What? **3**

2 It is About People **7**

2.1 Human and Social Issues 7
Markus Jakobsson

2.1.1 Nigerian Scams 8
2.1.2 Password Reuse 9
2.1.3 Phishing 11

2.2 Who are the Criminals? 13
Igor Bulavko

2.2.1 Who are they? 13
2.2.2 Where are they? 14
2.2.3 Deep-Dive: Taking a Look at Ex-Soviet Hackers 14
2.2.4 Let's try to Find Parallels in the World we Live in 16
2.2.5 Crime and Punishment? 16

3 How Criminals Profit **19**

3.1 Online Advertising Fraud 20
Nevena Vratonjic, Mohammad Hossein Manshaei, and Jean-Pierre Hubaux

3.1.1 Advertising on the Internet 20
3.1.2 Exploits of Online Advertising Systems 23

3.1.3 Click Fraud 25
3.1.4 Malvertising: Spreading Malware via Ads 31
3.1.5 Inflight Modification of Ad Traffic 32
3.1.6 Adware: Unsolicited Software Ads 34
3.1.7 Conclusion 35
3.2 Toeing the Line: Legal but Deceptive Service Offers 35
Markus Jakobsson and Ruilin Zhu
3.2.1 How Does it Work? 36
3.2.2 What do they Earn? 36
3.3 Phishing and Some Related Attacks 38
Markus Jakobsson and William Leddy
3.3.1 The Problem is the User 38
3.3.2 Phishing 38
3.3.3 Man-in-the-Middle 39
3.3.4 Man-in-the-Browser 40
3.3.5 New Attack: Man-in-the-Screen 41
3.4 Malware: Current Outlook 42
Members of the BITS Security Working Group and staff leads Greg Rattray and Andrew Kennedy
3.4.1 Malware Evolution 42
3.4.2 Malware Supply and Demand 48
3.5 Monetization 53
Markus Jakobsson
3.5.1 There is Money Everywhere 53

4 How Things Work and Fail 57

4.1 Online Advertising: With Secret Security 58
Markus Jakobsson
4.1.1 What is a Click? 58
4.1.2 How Secret Filters are Evaluated 60
4.1.3 What do Fraudsters Know? 62
4.2 Web Security Remediation Efforts 63
Jeff Hodges and Andy Steingruebl
4.2.1 Introduction 63
4.2.2 The Multitude of Web Browser Security Mechanisms 64
4.2.3 Where do we go from Here? 75
4.3 Content-Sniffing XSS Attacks: XSS with Non-HTML Content 75
Juan Caballero, Adam Barth, and Dawn Song
4.3.1 Introduction 75
4.3.2 Content-Sniffing XSS Attacks [illegible]

4.3.3 Defenses 84
4.3.4 Conclusion 89

4.4 Our Internet Infrastructure at Risk 89
Garth Bruen

4.4.1 Introduction 89
4.4.2 The Political Structure 90
4.4.3 The Domain 92
4.4.4 WHOIS: Ownership and Technical Records 94
4.4.5 Registrars: Sponsors of Domain Names 96
4.4.6 Registries: Sponsors of Domain Extensions 97
4.4.7 CCTLDs: The Sovereign Domain Extensions 99
4.4.8 ICANN: The Main Internet Policy Body 100
4.4.9 Conclusion 102

4.5 Social Spam 103
Dimitar Nikolov and Filippo Menczer

4.5.1 Introduction 103
4.5.2 Motivations for Spammers 105
4.5.3 Case Study: Spam in the GiveALink Bookmarking System 108
4.5.4 Web Pollution 114
4.5.5 The Changing Nature of Social Spam: Content Farms 116
4.5.6 Conclusion 117

4.6 Understanding CAPTCHAs and Their Weaknesses 117
Elie Bursztein

4.6.1 What is a Captcha? 117
4.6.2 Types of Captchas 118
4.6.3 Evaluating Captcha Attack Effectiveness 118
4.6.4 Design of Captchas 119
4.6.5 Automated Attacks 124
4.6.6 Crowd-Sourcing: Using Humans to Break Captchas 127

4.7 Security Questions 131
Ariel Rabkin

4.7.1 Overview 131
4.7.2 Vulnerabilities 134
4.7.3 Variants and Possible Defenses 138
4.7.4 Conclusion 139

4.8 Folk Models of Home Computer Security 140
Rick Wash and Emilee Rader

4.8.1 The Relationship Between Folk Models and Security 140
4.8.2 Folk Models of Viruses and Other Malware 142
4.8.3 Folk Models of Hackers and Break-Ins 146
4.8.4 Following Security Advice 149
4.8.5 Lessons Learned 153

4.9 Detecting and Defeating Interception Attacks Against SSL 154
Christopher Soghoian and Sid Stamm

4.9.1 Introduction 154
4.9.2 Certificate Authorities and the Browser Vendors 155
4.9.3 Big Brother in the Browser 157
4.9.4 Compelled Assistance 158
4.9.5 Surveillance Appliances 159
4.9.6 Protecting Users 160
4.9.7 Threat Model Analysis 163
4.9.8 Related Work 166
4.9.9 Conclusion 168

5 The Mobile Problem 169

5.1 Phishing on Mobile Devices 169
Adrienne Porter Felt and David Wagner

5.1.1 The Mobile Phishing Threat 170
5.1.2 Common Control Transfers 172
5.1.3 Phishing Attacks 178
5.1.4 Web Sender ⇒ Mobile Target 182
5.1.5 Web Sender ⇒ Web Target 184
5.1.6 Attack Prevention 185

5.2 Why Mobile Malware will Explode 185
Markus Jakobsson and Mark Grandcolas

5.2.1 Nineteen Eighty-Six: When it all Started 186
5.2.2 A Glimpse of Users 186
5.2.3 Why Market Size Matters 186
5.2.4 Financial Trends 187
5.2.5 Mobile Malware Outlook 187

5.3 Tapjacking: Stealing Clicks on Mobile Devices 189
Gustav Rydstedt, Baptiste Gourdin, Elie Bursztein, and Dan Boneh

5.3.1 Framing Attacks 189
5.3.2 Phone Tapjacking 191
5.3.3 Framing Facebook 194
5.3.4 Summary and Recommendations 195

6 The Internet and the Physical World 197

6.1 Malware-Enabled Wireless Tracking Networks 197
Nathaniel Husted and Steven Myers

6.1.1 Introduction 198
6.1.2 The Anatomy of a Modern Smartphone 199