

The book cover features a blue-toned globe with a grid of latitude and longitude lines. The globe is set against a background of binary code (0s and 1s) that appears to be falling or floating. A white banner with a downward-pointing arrow shape is positioned at the top, containing the title text. The text is in a bold, blocky, sans-serif font. The words are stacked vertically, with horizontal lines separating the second and third lines, and the fourth and fifth lines.

CYBERATTACK
CYBERCRIME
CYBERWARFARE
CYBERCOMPLACENCY

MARK OSBORNE

CYBERATTACK

CYBERCRIME

CYBERWARFARE

CYBERCOMPLACENCY

IS HOLLYWOOD'S BLUEPRINT FOR CHAOS COMING TRUE



MARK OSBORNE

Copyright © 2013 Mark Osborne

All rights reserved.

ISBN: 1493581287

ISBN 13: 978-1493581283

Library of Congress Control Number: 2013920296

CreateSpace Independent Publishing Platform

North Charleston, South Carolina

PREFACE

Blanche DuBois:

“I have always depended on the kindness of strangers.”

Streetcar Named Desire (1947)

Like the quote above—stranger, please be kind!!! Time (contrary to the song) wasn't on my side when I wrote this book. I tried hard to maintain a jovial style to help you enjoy it, but this could be my epitaph, my legacy, if you will. I couldn't afford to linger on every page because I was actually concerned that I might snuff-it and depart this mortal coil.

So here's the deal: just less than two years ago, I was the loud, fat, and obnoxious, yet usually right, security bloke that many of you in the UK security industry are probably familiar with. Despite the best available medical indifference (you have to make a joke, don't you!), I went into septic shock and had a twenty-by-twenty-inch alien mass, along with a two foot section of my gut and a lump of my spleen, removed. To save anyone any trouble or inconvenience, I slipped into a *coma*. It kept me nice and quiet.

And here's the clincher!! The excellent chief surgeon and other wonderful lung specialist that saved me say that most of my bits and pieces are fixed, but with the caveat that I am only here out of an act of sheer bloody-mindedness. The episode has reduced my MTTF ("Mean-Time To Failure"). Judging by the pain and the screaming headache I get at the end of each working day, I tend to agree with them (but hey, dear reader, I bet that many of you have jobs that do the same thing to you despite your good health). However, my General Practitioner (GP) sniffs and says I'm all fixed—but bear in mind that this is the same guy that missed all the symptoms in the first place. This presents a dilemma but all things considered I think you'll understand why I "felt pressed" to finish the book.

Please be kind!! With my other whitepapers, books, exploits, and software I have noticed a trend. There are always comments on newsgroups or forums that say that:

- "They" could solve a 10GB/s SynFlood by using a laptop with a 486 cpu, 100Mb Ethernet card, and the netstat command
- "They" could have discovered the *zero-day* themselves if only they had looked
- "They" could have produced a much better IDS than me—if they only had the time, could write C, knew about device drivers, and had a computer ("Oh, by the way, before I start, can you remind me what an IDS does?")

"Woulda! Coulda! Shoulda!" or as my granny used to say, "If *'ifs and ands'* were *'pots and pans,'* there'd be no work for tinkers' hands."

So if you are that guy, *be* kind. If you notice a mistake, email me, and if you don't like it, let's keep it a secret—it can be our own *zero-day*, our own special thing. Please don't share it with the world. If you feel so negatively about my book, maybe you should just write a better one.

Having said that, if you love this book then tell everyone, write great reviews, and buy ten copies of it. Marge, the kids and the charities that will benefit from sales will appreciate it. That being said, nobody writes a security book or publishes open-source security tools for the money—I do it because it entrances me; I am bewitched.

So what's the book about, you ask? Please consider for a moment this statement made by J. Saiteerdou, Head of Computer Crimes at the FBI: "Give me ten carefully chosen hackers, and within ninety days I would then be able to have this nation lay down its arms and surrender."

At first glance, that about sums up the book—or at least my intent when I started it. A while ago, I realised that a *digital attack* could easily cripple a country like the UK, especially if the attackers have the resources of a sovereign power supporting them. If they don't have such resources, a blended attack which combined digital attacks with physical attacks could still be as effective. There seems to be so little public awareness about how real this possibility is and how it could come about, I felt the need to communicate what information I have gathered on this subject.

This isn't a "how-to" book and is rather designed to provide business insights into the field of digital security for the more technical people. It also provides concrete and easy-to-follow technical examples for business people who may be unfamiliar with all the technical references.

New Media

Modern media is ubiquitous and all-encompassing, spread over a wide variety of digital channels. I have tried to embrace this, as it is in-keeping with the theme of the book. I have provided:

- example code and exploits on *packetstorm* (*dns_spquery.c* & *obeseus.c*)
- example and supporting Android Apps on Google *Play*
- code and "config" files on my usual site www.loud-fat-bloke.co.uk
- presentations and lectures on *FaceBook*

I have already presented some of these at public events; if you get a chance to come and see me, you are more than welcome – Likewise, if you are hosting an event. I am much better live (over 18s only).

Much Thanks

Lastly, thanks to...well...everybody who helped.

And as a postscript, thanks to the ever-so-nice editor bloke, Dave, who gently helped some of it make sense and also curbed my natural laddish enthusiasms by removing the woefully inappropriate expression of my appreciation for “big guns” and “Sandra Bullock”. Like they say, you can lead a horse to water!

TABLE OF CONTENTS

Preface	iii
Chapter 1: The Introduction	1
1 Introduction	3
2 The Government Will Protect Me, But from What?	5
3 What <i>Isn't</i> Cyber Security?	10
Chapter 2: The Internet is a Business——Understanding the E-Economy Platform	13
1 Introduction	13
2 Cyberspace and the Internet	14
3 The Internet as a Business	14
4 What is an ISP's Core Business	21
5 A Hierarchy of Clouds.....	22
6 Peering.....	24
7 Routing and Economics.....	25
8 Security Services on Peering and Transit Traffic.....	28
9 The Exchange-Based Interconnection Model.....	29
10 Subsea Cables	30
11 Summary	30
Chapter 3: Who Monitors the Internet	33
1 Situation Report	33
2 Players distribute attack information collected by others	35
3 Players that Monitor Attacks and Analyze Traffic.....	46
4 Analysis.....	49
5 Summary	53

Chapter 4: Monitoring Tools and Techniques	57
1 Firewall-Log Suckers.....	58
2 Honeypot	58
3 Darknet	61
4 Network Telescopes.....	61
5 NetFlow	64
6 Monitoring Cyber-Security Traffic Without Guessing.....	69
7 Summary	72
Chapter 5: Hardware Architecture of a Probe	75
1 The Speed Dilemma	75
2 Requirements	77
3 Strategies for 10Gb/s or 40Gb/s.....	78
4 A Third Way: The Chosen Approach.....	80
5 Now with Computer Science on Our Side.....	82
6 In Detail	85
7 Summary.....	88
Chapter 6: Software Architecture of a Probe	91
1 Introduction	91
2 Why Most Products Don't Cut It	92
3 Probe Design	94
4 Layer 1—FPGA Network Packet Processor.....	96
5 Layer 2—BUS Layer	98
6 Layer 3—Packet Decode Layer.....	98
7 Additional Post-Processing Layers.....	102
8 Potential Improvements.....	103
9 Summary.....	103
Chapter 7: Types of DDOS Attack	105
1 The Evolution of the Denial of Service Attack.....	105
2 Denial of Service.....	106

3	Resource Overload	107
4	Attacks with a Single Payload that Causes Failure	112
5	Application Attacks	113
6	The DDOS Attacks	113
7	The Economics of DDOS.....	118
8	Attack Strength of DDOS.....	120
9	Summary	121
Chapter 8: DDOS Detection.....		123
1	DDOS Detection.....	123
2	Per-Link/Per-Subnet Traffic Profile	124
3	Attack Signatures.....	125
4	Protocol Analysis	125
5	Determining the Target	126
6	Protocol Analysis	127
7	Other Techniques.....	132
8	Summary	133
Chapter 9: DDOS Mitigation.....		135
1	Key Features of an IDMS.....	136
2	DDOS Historic Prevention, Reactions, and Remediation	136
3	RFC2827.....	137
4	Blacklist.....	141
5	More from Space–Black Holes	143
6	Committed Access Rate Acls.....	146
7	Synproxies.....	147
8	Pull Up the Drawbridge and Defend the Fort.....	149
9	Scatter, Divide, and Conquer–AKAMAI.....	158
10	Summary.....	160
Chapter 10: Cyber-Attack Case Study		163
1	The Chronology	164

2	Unrestricted Warfare—a New Blueprint for War?	172
3	Summary	175
Chapter 11.0: The Weak Points.....		177
Chapter 11.1: Physical Vulnerabilities		179
1	Physical Assets	180
2	Premises/Buildings	181
3	Interconnections	185
4	Operations	191
5	Summary	193
Chapter 11.2: BGP Vulnerabilities		195
1	BGP Insecurity	195
2	DOS the Router Causing a Route FLAP	196
3	A Hacker Attacking a Peering Router	197
4	BGP Stealing a Subnet with AS and Router.....	202
5	Subverting a Route Path with a Rogue AS and Router	209
6	Summary	218
Chapter 11.3: DNS Vulnerabilities.....		221
1	Flooding Key DNS Servers	222
2	Query Redirection.....	222
3	DNS Cache-Poisoning Attack.....	225
4	DNS Snooping	226
5	DNS Fast Flux	229
6	DNS DDOS Reflector Attacks:	230
7	DNS Recommendation	235
8	Summary	236
Chapter 11.4: The Software Threat		239
1	This Chapter:	240
2	The Maths	240
3	Malware	241

4	AV Protection.....	243
5	The Software Robot Army—a Functional Comparison	245
6	Cyber War: When Good Software Turns Bad	251
7	Cyber War: When Software Starts Out Bad.....	255
8	Summary	255
Chapter 11.5: A Growing Zombie Army.....		257
1	The Enemy at the Gate	257
2	Traditional View	258
3	Zombies are Walking.....	258
4	IPv6.....	259
5	Summary	261
Chapter 11.6: ICS and SCADA.....		263
1	Terminology.....	263
2	The Underlining Reasons for Insecure ICS	265
3	Typical System: System Security Characteristics Profile	266
4	Security Profile of the Target.....	267
5	Authentication.....	267
6	Protocols	268
7	Carrier	270
8	Encryption	270
9	Vulnerability and Exposure Time.....	271
10	Fragility and Resilience	271
11	Security Logging and Alerting.....	272
12	Bottom Line: Less Secure Than Other Internet Facing Systems ...	272
13	SCADA/ICS Case Studies	273
14	Attack Descriptions	275
15	Stuxnet Case Study.....	278
16	Getting to Them.....	280
17	Summary	280

Chapter 12: The Fire Sale: Hollywood’s Blueprint for Chaos.....	283
1 Fire Sale Step 1 of DH4’s Plan–Blocking Transport Links.....	285
2 Step 2: The Financial Base and Telecoms.....	287
3 Step 3: The Rest.....	290
4 And Now the Clever Stuff	291
5 Fin.....	292

CYBER CYBER WAR

Biblioteka Główna
Akademii Sztuki Wojennej

26619/III (CB)



03-026619-000-0

?

Is Hollywood's I

Will hackers or hacktivists shut down the banks, the gas and the electricity supply—Can terrorists invade cyberspace, then use malware and BotNets to put an “out of lunch” sign on UK PLC. What are the techniques used to detect this type of attack and do those in power have a clue about the exposure.

Mark Osborne, also known as loud-fat-bloke, will explain all – After a lifetime of running the cyber security functions at the largest Security Consulting, ISPs and Technology providers, he designed Europe's largest cyber-monitoring system and has managed his way out of more than his fair share of Cyberattacks.

In this book, armed by real world experience, Osborne shows how exposed we all really are.

The Book covers:

- Economics of cyberspace and cyber-security.
- Who's monitoring cyberspace and Why.
- The monitoring techniques used and why they fail to protect the general population from Cyber- attack.
- How to detect, mitigate and measure the cost of a DDOS attack.
- The mechanics of BotNets and their C&C servers.
- How to exploit vulnerabilities in the Physical, BGP, DNS, IPV6 and SCADA components of the Internet & cyberspace.
- Finally, it describes a “Fire-sale” where all these techniques are used to turn off the gas, electric and all the lights just like in the movies.

What they say about the author:

“Osborne is one of the most charismatic and blatantly funny people you could hope to meet.”

Communication News

“One for the bookshelf”

Information Security Magazine

“Mark Osborne's article was a useful resume on this important subject (internet Security)”

Buckingham palace

“An informative and often entertaining introduction to information security...
an informative and valuable read.”

****(four stars) *SlashDot/ Ben Rothke*

Osborne's last book “How To Cheat at Managing Information Security” reached the Amazon.com Top-500. It has consistently appeared as 1st in category since publication.

About the Author

Mark Osborne has held Security leadership roles at KPMG, Interoute and HP/T-Systems. This gave him daily exposure to large scale cyber-attacks. He never forgot his software/security engineering background which included penetration testing, developing Zero-Day security vulnerabilities, coding exploits and creating open source mitigation tools like IDS/IPS. Most pertinently he designed and coded one of the largest Cyber Security System in the world to detect cyber-attacks.

ISBN 9781493581283

9"781493"581283"