

Contents

Preface	_____	vii
Introduction	_____	1
1 Physical Security	_____	15
1.1	Side-Channel Attacks	15
1.2	Physical Threats	20
1.3	Laptop Security	26
1.4	Disaster Recovery Planning	28
1.5	Privacy Protection	29
2 Viruses	_____	33
2.1	Operating Systems	34
2.2	Computer Viruses	36
2.3	Virus Writers	40
2.4	Virus Propagation	43
2.5	Virus Classification	46
2.6	Boot Sector Viruses	48
2.7	File Infector Viruses	51
2.8	Companion Viruses	55
2.9	Multipartite Viruses	56
2.10	Macro and Script Viruses	57
2.11	Infected Images	59
2.12	Virus Life Cycle	62
2.13	Viruses and UNIX	65
2.14	Viruses and the Macintosh	65
2.15	Viruses and the Amiga	66
2.16	Virus Replication	66
2.17	Virus Payload	66
2.18	Virus Organization	74
2.19	Virus Naming	75

xx Contents

2.20	Virus Hiding Methods	76	
2.21	Polymorphism	80	
2.22	Virus Stealth Techniques	83	
2.23	Interrupts and Viruses	84	
2.24	Trapdoors	88	
3	Worms		91
3.1	Code Red I	93	
3.2	Worming Techniques	95	
3.3	Proposing a CCDC	105	
3.4	The Internet Worm	108	
4	Trojan Horses		113
4.1	Applications of Trojans	114	
4.2	Installing a Trojan	116	
4.3	Rigging a Compiler	118	
5	Examples of Malware		125
5.1	The Lehigh Virus	125	
5.2	The Brain Virus	126	
5.3	The Michaelangelo Virus	127	
5.4	The SirCAM Virus	128	
5.5	The Melissa Virus	129	
5.6	Scores Virus	130	
5.7	Swiss Amiga Virus	131	
5.8	Christmas Card Virus	131	
5.9	VBS.KAK Worm	132	
5.10	The Cruncher Virus	133	
5.11	Opener Virus	134	
5.12	MTX Worm/Virus	135	
6	Prevention and Defenses		139
6.1	Understanding Vulnerabilities	139	
6.2	Defenses Against Malware	144	
6.3	Anti-Virus Software	145	
6.4	Backups and Such	155	
6.5	Hoaxes	160	
7	Network Security		163
7.1	Internet Vulnerabilities	163	
7.2	Port Scanning	164	
7.3	Spoofs	165	
7.4	Spam	169	
7.5	Denial of Service	181	
7.6	Firewall Basics	184	
8	Authentication		189
8.1	Local Authentication	190	
8.2	Biometric Techniques	190	
8.3	Passwords	196	

9	Spyware _____	211
9.1	Introduction and Definition	212
9.2	RIAA and Spyware	215
9.3	Terrorism and Spyware	217
9.4	Political Contributions	218
9.5	Distribution of Spyware	219
9.6	Remote Reporting	222
9.7	Adware	225
9.8	Spyware?	226
10	Identity Theft _____	231
10.1	Introduction	232
10.2	Shredding	236
10.3	Internet Cookies	238
10.4	Phishing	239
10.5	The Homograph Threat	245
11	Privacy and Trust _____	247
11.1	Privacy Issues	248
11.2	Online Privacy	251
11.3	Children’s Privacy	253
11.4	Trust	258
12	Elements Of Cryptography _____	263
12.1	Principles of Cryptography	264
12.2	Kerckhoffs’s Principle	265
12.3	Polybius’s Monoalphabetic Cipher	266
12.4	Polybius’s Polyalphabetic Cipher	268
12.5	The One-Time Pad	269
12.6	The Key Distribution Problem	271
12.7	Diffie–Hellman–Merkle Keys	272
12.8	Public-Key Cryptography	273
12.9	RSA Cryptography	274
12.10	SSL: Secure Socket Layer	278
A	l33t Speak _____	285
B	Virus Timeline _____	289
	Concluding Remarks _____	305
	Answers to Exercises _____	311
	Glossary _____	327
	Bibliography _____	343
	Index _____	357

LIFF (n.). A book, the contents of which are totally belied by its cover. For instance, any book the dust jacket of which bears the words. “This book will change your life.”

—Douglas Adams, *The Meaning of Liff* (1984)