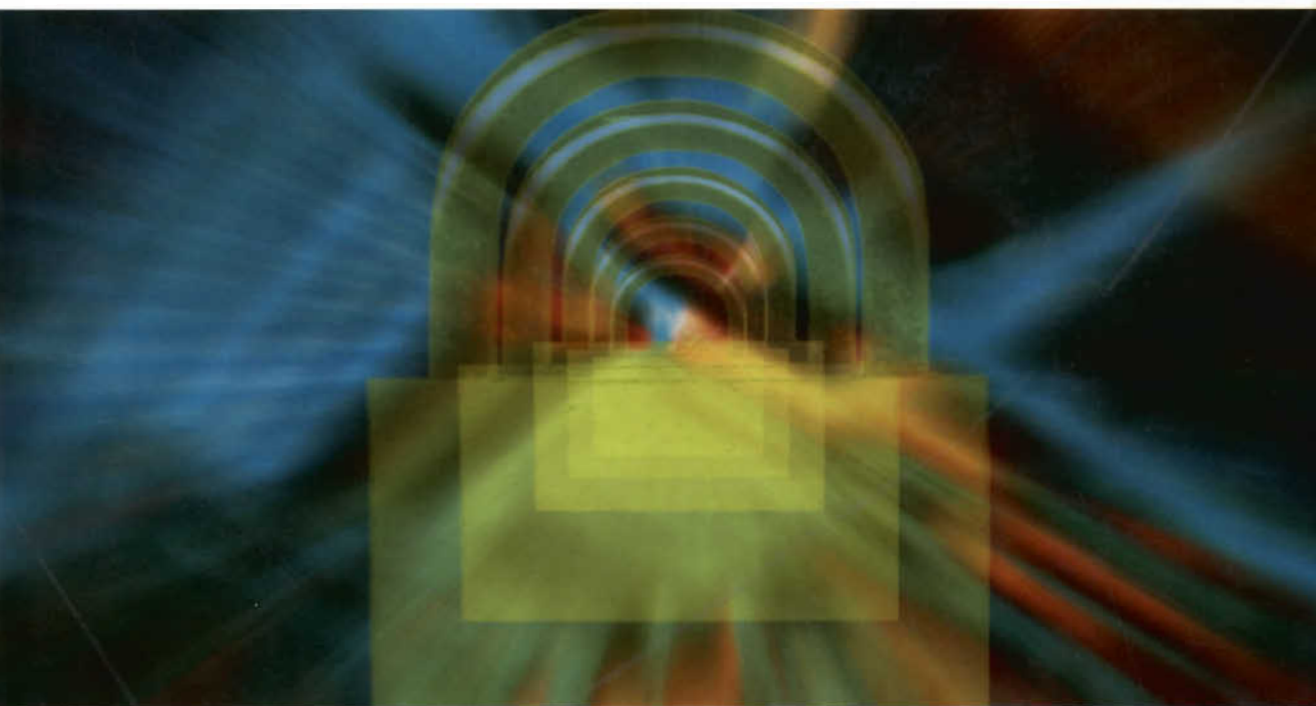


Internet Security

Risk Analysis, Strategies and Firewalls



CD-ROM



INCLUDED

Includes **WebExtraSM**
added value online

Othmar Kyas



Internet Security

Risk Analysis, Strategies and Firewalls

Othmar Kyas



International Thomson Computer Press



An International Thomson Publishing Company

London • Bonn • Boston • Johannesburg • Madrid • Melbourne • Mexico City • New York • Paris
Singapore • Tokyo • Toronto • Albany, NY • Belmont, CA • Cincinnati, OH • Detroit, MI

Contents

	Foreword	xiii
Chapter 1	Internet security: risk analysis	I
1.1	The Internet as a security risk: Hazard on the information highway?	1
1.2	Basic risks to the DP infrastructure	2
1.3	Being on the Internet: the risks	3
1.4	Internet: risk analysis	4
1.5	Detailed risk analysis	10
Chapter 2	Computer crime: who does it and why	13
2.1	Who could be out to get you?	13
2.2	Hackers from college	14
2.3	Staff: the threat from within	14
2.4	Hackers from the computer underground	15
2.5	Old-fashioned criminals: drugs and the Mafia	19
2.6	Cybercrime: professional hackers	19
2.7	The danger is growing	20

Chapter 3	Hackers and viruses: the first 30 years	21
3.1	The telephone hackers of the 1960s and 1970s	21
3.2	The first hackers	23
3.3	Underground mailboxes (BBS)	25
3.4	The professional hackers of the '90s	27
Chapter 4	Internet security: attack points and weaknesses	31
4.1	Potential security gaps in networks	31
4.2	Internet: faulty software design	31
4.3	Company organization as security risk	32
4.4	Hit list of hacking methods	33
4.5	Threats to Internet clients	34
Chapter 5	Access control as a security risk (authentication)	35
5.1	Capturing passwords	35
5.2	"Soft" passwords	38
5.3	Choosing passwords	40
5.4	Protecting your "passwd" file	42
5.5	Analyzing protocols and filtering passwords (sniffer attacks)	43
5.6	Password monitoring with TRSR programs	44
5.7	Fishing for passwords with "Trojan horses"	44
5.8	Smart cards	45
Chapter 6	Communications protocols as security risks	47
6.1	Communication protocols on the Internet	48
6.2	Security problems and attacks via Internet protocols	52
Chapter 7	Internet applications: the risks	65
7.1	Managing TCP/IP Internet applications	65
7.2	Hacking via remote login	67
7.3	The DNS service	69
7.4	SMTP as a safety risk	72
7.5	Security risks: file transfer	78
7.6	NFS (Network File System)	80
7.7	NIS attacks	81
7.8	NTP attacks	82
7.9	Security gaps in the X.11/X-Windows system	82

7.10	Critical Internet applications: finger and whois	87
7.11	NNTP (The Network News Transport Protocol)	88
7.12	EGP (Exterior Gateway Protocol)	89
Chapter 8	Information services as security risks: WWW, Gopher, FTP	91
8.1	Setting up information servers	92
8.2	Gopher servers: security risks	93
8.3	WWW servers: security risks	96
8.4	Configuring secure WWW server systems	100
8.5	The security risks in anonymous FTP servers	101
Chapter 9	Viruses in programs and networks	105
9.1	Different kinds of viruses	106
9.2	Virus factories	109
9.3	Anti-virus management	109
9.4	Anti-virus consultants	110
9.5	Anti-virus software	111
9.6	Anti-virus newsletters	112
Chapter 10	Internet security: design and implementation	115
10.1	Corporate guidelines for network security	115
10.2	Implementing an Internet security architecture	124
Chapter 11	Firewalls: architecture and function	127
11.1	Firewalls: definition and philosophy	127
11.2	Firewalls: main design features	128
11.3	The architecture of firewall systems	132
11.4	The limits of firewalls	138
Chapter 12	Packet filter-based firewalls	139
12.1	Bridges in networks	139
12.2	Linking networks via routers	140
12.3	Routers as packet filter firewalls	143
12.4	How packet filters works	142
12.5	Planning the packet filter configuration	147
12.6	Setting up filters: strategies and models	148

	12.7	Topology of packet filter firewalls bastion host}	152 155
	12.8	Filtering Internet connections: TCP Wrapper and Port Mapper	156
	12.9	Internal firewalls	157
	12.10	Internet directory	157
Chapter 13		Circuit relay and application gateway firewalls	159
	13.1	Proxy server	159
	13.2	Circuit relays	160
	13.3	SOCKS clients for the DOS/Windows platform	165
	13.4	UDP relays	166
	13.5	IP emulators	166
	13.6	Application gateways	166
Chapter 14		Cryptography: secure communications via insecure networks	169
	14.1	DES (Data Encryption Standard) the symmetrical encryption process	170
	14.2	Public key encryption methods (asymmetrical encryption)	171
	14.3	Export controls and patents on encryption systems	175
	14.4	PEM, the Internet e-mail encryption standard	178
	14.5	Digital signatures	179
	14.6	Message digests: file integrity	180
Chapter 15		Attack simulators	181
	15.1	Attack simulators	181
	15.2	System security check software	184
	15.3	Other watching tools	186
	15.4	Intrusions Detection Systems (IDS)	187
Chapter 16		Network security: standards and organizations	189
	16.1	The Orange Book (TCSEC)	190
	16.2	The ITSEC standard catalogue for Europe	193
	16.3	NIST (National Institute of Standards and Technology)	194
	16.4	NSA (National Security Agency)	195

Chapter 17	Internet Security: useful online information	197
17.1	Information servers on Internet security	197
17.2	Information on the computer underground	199
17.3	Newsletters and mailing lists	200
17.4	Underground journals and magazines	202
17.5	Newsgroups on Internet security	203
Chapter 18	Firewalls: trends and future development	205
18.1	ATM firewalls	205
18.2	Firewalls and detecting attacks using artificial intelligence	206
18.3	The post-firewall era	206
Appendix A	Organizations	207
Appendix B	Reports, archives, mailing lists, newsletters	211
Appendix C	Guidelines, legislation	215
Appendix D	Requests for Comments (RFCs) of relevance to security: index	219
Appendix E	Internet directory	225
Appendix F	Viruses	259
Appendix G	CD-ROM: Firewall toolkit	271
Appendix H	Producers and Manufacturers	279
Appendix I	Sources	285
	Index	289

Internet Security

Risk Analysis, Strategies and Firewalls

Othmar Kyas

The Internet is an open network, which means everyone can have access to it, like a public park, museum or monument. In common with other public places, it has the potential disadvantage of lack of security, which is of great concern to most businesses, governments and some individuals.

This book gives a concise, readable overview of Internet security. In particular, it will help network and IT managers and systems administrators understand the importance of security, how to evaluate their security needs and how to implement the best solutions through in-depth risk analysis and the development of a corporate security strategy. Numerous real-world examples are also provided throughout the book.

Internet Security:

- Provides a systematic approach to developing and implementing an Internet security architecture, with special attention given to in-depth risk analysis and corporate security strategy development, which will be of particular importance to network managers, systems administrators and others who manage and make strategic decisions regarding the use of the Internet.
- Contains an analysis of potential criminal profiles as well as detailed numbers and statistics on computer crime on the Internet.
- Describes in detail various attack techniques used by hackers from the Internet.
- Includes Firewalls and security tools on CD-ROM with software and documentation on Internet security.
- Runs on PC and UNIX systems.

ABOUT THE AUTHOR

Othmar Kyas has worked for Hewlett-Packard in Germany since 1989 as a specialist in data and telecommunications. He is author of *ATM Networks, Second Edition*, and the forthcoming *Fast Ethernet, Token Ring and Segment Switching*, and is also coauthor of *Troubleshooting LANs*, all published by International Thomson Computer Press.



ISBN 1-85032-302-X



9 781850 323020



Includes WebExtraSM
added value online

Printed in the USA