

Contents

1	Introduction	1
	1.1 Preamble.....	1
	1.2 What is a Computer Virus?.....	1
	1.3 Worms: Networked Viruses.....	2
	1.4 Terminology.....	3
2	Historical Perspectives	5
	2.1 Introduction.....	5
	2.2 1960s: Early Rabbits.....	5
	2.3 1970s: Fiction and the Worm.....	6
	2.4 1980–1983: Genesis.....	8
	2.5 1984–1986: Exodus.....	10
	2.6 1987: Mac, Atari and Amiga Next.....	12
	2.7 1988: Proliferation and Disbelief.....	14
	2.7.1 January–March.....	14
	2.7.2 April–September.....	15
	2.7.3 October–December.....	16
	2.8 1989: Reaction by the Community.....	19
	2.8.1 January–March.....	19
	2.8.2 April–June.....	20
	2.8.3 July–September.....	22
	2.8.4 October–December.....	24
	2.9 1990: Organisation and Litigation.....	27
	2.9.1 January–April.....	27
	2.9.2 May–September.....	28
	2.9.3 October–December.....	29
	2.10 Summary.....	30
3	Theory of Viruses	31
	3.1 Introduction.....	31
	3.2 Addition of Viral Code.....	31
	3.3 Detection of Viruses.....	35
	3.4 Classes of Viruses.....	36
	3.5 Thompson: and Trusting Trust.....	38

3.6 Biological Analogies	42
3.6.1 Biological Viruses	43
3.6.2 Parallels Between Low Level Operation	44
3.6.3 High Level Parallels	45
3.7 Quest for Life	46
3.8 Evolution: Genetic Algorithms	48
3.8.1 Random Mutation	48
3.8.2 Programmed Mutation	48
3.8.3 Genetic Algorithms	50
3.8.4 Growth and Death	51
4 Operation of PC Viruses	55
4.1 Introduction	55
4.2 PC Boot Sequence: Initialisation	56
4.3 BIOS and DOS	56
4.4 Master Boot Record	57
4.5 DOS Boot Sector	58
4.6 System Initialisation	59
4.7 Batch Processing Viruses	60
4.8 COM and EXE Viruses	61
4.8.1 Non-overwriting Prepending COM Infectors ...	62
4.8.2 Overwriting COM Infectors	63
4.8.3 Non-overwriting Appending COM Infectors ...	63
4.8.4 EXE Viruses	64
4.9 Resident and Transient Viruses	65
4.10 Manipulation by Viral Code	69
4.11 Activation Criteria	70
4.12 Camouflage	73
4.12.1 Concealment in Infected Files	74
4.12.2 Encryption of Viral Code	74
4.12.3 Hiding of Viral Code	77
4.12.4 Checksum Calculation	78
4.12.5 Prevention of Alteration Detection	78
4.12.6 Concealment of Viral Code in Memory	79
4.12.7 Concealment of Viral Activity	80
4.12.8 Concealing Disk Activity	82
4.12.9 Concealing System Slowdown	82
4.13 Replication	83
4.13.1 Locating a Host	83
4.13.2 Signatures	84
4.13.3 Miscellaneous Topics	86
4.13.3.1 Corresponding File Virus	86
4.13.3.2 SYS Virus	87
4.13.3.3 Multi-vector Viruses	87
4.13.3.4 Multi-architecture Viruses	87
4.13.3.5 Architecture Dependent Viruses	88

5	Management of PC Viruses	91
5.1	Perspective on Security	91
5.2	Components of a Virus Control Scheme	91
5.3	Prevention of Virus Attack	92
5.3.1	Physical Access Constraints	93
5.3.2	Electronic Measures	94
5.3.2.1	Physical Feature Verification	95
5.3.2.2	Knowledge Verification	95
5.3.2.2.1	Passwords	96
5.3.2.2.2	Background Verification	97
5.3.2.2.3	Other Techniques	97
5.3.2.3	Possession Verification	97
5.3.3	Media Access Controls	97
5.3.4	Network Access Controls	98
5.3.4.1	Identification of Access Controls	99
5.3.4.1.1	Centralised Network File Servers	99
5.3.4.1.2	Distributed Trust	100
5.3.4.1.3	Network Transport by Public Carrier or Accessible Media	100
5.3.5	Ideological Controls	101
5.3.5.1	User Education	101
5.3.6	Management Policies	105
5.3.6.1	Training of Employees	105
5.3.6.2	Use of Anti-viral Measures	105
5.3.6.3	Compartmentalisation	107
5.3.6.4	Centralisation	107
5.3.6.5	Personnel Policies	108
5.3.7	Vaccination and Inoculation	108
5.4	Detection of Viral Code	109
5.4.1	Monitoring and Logging	109
5.4.2	Signature Recognition	112
5.4.3	Generic Code Recognition	112
5.4.4	Sacrificial Lamb	114
5.4.5	Auditing	115
5.4.6	Use of Expert Systems to Analyse Viral Behaviour	116
5.4.7	Fighting Fire with Fire	117
5.5	Containment of Viral Code	118
5.5.1	Hardware Compartmentalisation	119
5.5.1.1	Virtual Machine	119
5.5.1.1.1	80386 Task Switching Support	120
5.5.1.1.2	80386 Paged Segmented Memory	120
5.5.1.1.3	Accessing OS Code	124
5.5.1.1.4	Segment Permissions	125
5.5.1.1.5	Paged Memory Operation	126

5.5.1.1.6	Input/Output Operations	127
5.5.1.1.7	Virtual Machine in Software.....	128
5.5.1.2	Automatic Flow Verification	129
5.5.1.3	Software Distribution: Ensuring Trust	130
5.5.2	Software Compartmentalisation	130
5.5.2.1	Interrupt Trapping Code	130
5.5.2.1.1	Configurable Monitors.....	131
5.5.2.1.2	Operation of a Monitor	133
5.5.2.1.3	Extensions to Real Time Monitoring	135
5.5.2.2	OS Support	135
5.5.3	Network Compartmentalisation	135
5.5.4	Investigation and Response	136
5.5.4.1	What is the Infection?.....	136
5.5.4.1.1	Acquisition	137
5.5.4.1.2	Logging of Relevant Information	138
5.5.4.1.3	Disassembly	138
5.5.4.2	Dissemination of Information	140
5.5.4.3	General Containment.....	141
5.5.4.4	Tracing of Infection Source.....	142
5.5.5	Disinfection of Viral Code.....	144
5.5.5.1	Re-installation	144
5.5.5.2	Recompilation from Source	145
5.5.6	Checking for Re-infection	145
5.5.7	Disinfection Utilities	146
5.6	Recovery from Viral Infection.....	147
5.6.1	Backup Procedures	147
5.7	Contingency Planning	148
5.7.1	Redundancy	149
5.7.2	Insurance	149
5.7.3	Public Relations	149
5.8	Remedial Action	150
6	Apple Macintosh Viruses	153
6.1	Introduction	153
6.2	Macintosh: The Abstract Operating System	154
6.2.1	Initialisation.....	156
6.2.2	Resources.....	158
6.2.3	Trap Dispatch Table Structure	161
6.2.4	Non-link Viruses	162
6.2.5	Link Viruses	162
6.2.6	Notes on Keyboard Sequences	165
6.2.7	Summary of Mac Protection.....	165
7	Mainframe Systems: The Growing Threat	167
7.1	Introduction	167
7.2	Hardware Architectures.....	167

7.3 Software Architecture	168
7.3.1 Discretionary Access Controls	168
7.3.2 Integrity versus Confidentiality	172
7.3.3 Mandatory Access Controls	173
7.3.4 Commentary on Security Standardisation.....	177
7.4 UNIX: A Viral Risk Assessment	180
7.4.1 System Startup	180
7.4.2 Login and User Commands	183
7.4.3 Bugs and Loopholes	184
7.4.4 Mechanics of UNIX Viruses	185
7.4.4.1 Batch Viruses	185
7.4.4.2 Link Viruses	186
7.4.4.3 Dynamic Loading	186
7.4.4.4 Other Considerations.....	186
7.4.4.5 Protecting Against UNIX Viruses	189
7.4.4.6 Cohen: Early UNIX Viruses	190
8 Network Viruses: The Worms	193
8.1 Introduction	193
8.2 Standardisation	194
8.3 History of Network Pests	195
8.3.1 Early Work: Pre-1980	195
8.3.2 Recent Benign and Malicious Worms	196
8.3.3 CHRISTMA EXEC Chain Letter	197
8.3.4 Chain Letters on UNIX	199
8.4 Internet Protocols	199
8.4.1 Architecture.....	200
8.4.2 Peer Authentication	201
8.4.3 Access Controls	202
8.4.4 Data Stream Integrity	202
8.4.5 Daemons and Servers	203
8.4.6 Distributed Trust	203
8.4.7 Trusted Ports	205
8.4.8 Problems and Solutions	205
8.4.9 Internet Worm: Black Thursday – 3 November 1988.....	205
8.4.9.1 Internals	206
8.4.9.2 Action and Reaction.....	208
8.4.9.3 The Aftermath	211
8.4.10 DISNET: A Child of the Internet.....	213
8.5 OSI: Security in the Making	214
8.6 DECNET: Insecurity Through Default.....	215
8.6.1 HI.COM: The Christmas Worm	216
8.6.1.1 Reaction of the DECNET Community	217
8.6.1.2 Worms Against Nuclear Killers	218

9	Reactions of the IT Community	221
	9.1 Discussion and Advice.....	221
	9.1.1 Bulletin Board and Casual Users	221
	9.1.2 Academic Establishments	222
	9.1.2.1 CREN/CSNET.....	223
	9.1.2.2 NSFNET	223
	9.1.2.3 HEPNET/SPAN	224
	9.1.2.4 General Community Responses	225
	9.1.3 Government Research Organisations.....	226
	9.1.4 Military Organisations	227
	9.1.5 Commercial Organisations	227
	9.1.6 Criminal Investigation Organisations	227
	9.1.7 Professional Organisations	227
	9.2 Legislative Issues.....	229
	9.2.1 Scottish Law Commission	230
	9.2.2 English Law Commission	231
	9.2.3 Computer Misuse Act.....	233
	9.2.4 Summary of Legislation	234
	9.3 Professionalism and Software Development	235
10	Conclusions: The Future Ahead.....	237
	Appendices	239
1	DOS Filestore Structure	239
	1.1 Introduction	239
	1.2 Master Boot Record	239
	1.3 DOS Boot Sector.....	240
	1.4 File Allocation Table.....	241
	1.5 Root Directory.....	242
2	Low Level Disk Layout	245
3	EXE File Format	249
4	Mac Filestore Structure	251
5	PC Virus Relationship Chart.....	253
6	Macintosh Virus Relationship Chart	255
7	PC Boot Sequence	257
8	AIDS Trojan: Accompanying Licence	259
9	Software Infected at Source	263

Contents	xiii
10 Nomenclature	265
10.1 Types of Virus	265
10.1.1 Master Boot Sector Viruses	265
10.1.2 DOS Boot Sector Viruses	265
10.1.3 Executable COM/EXE Viruses	265
10.1.4 Memory Resident Viruses	266
10.1.5 Overwriting Viruses	266
10.1.6 Prepending Viruses	266
10.1.7 Appending Viruses	266
10.2 Generations of Virus	266
10.3 Classes of Anti-virus Product	267
11 UNIX Boot Sequence	269
12 CERT Press Release	271
13 CERT/CIAC Advisories	273
14 Contact Points	277
15 Abbreviations	279
16 Further Reading	283
17 Virus-l Archive Sites	291
18 Relative Frequencies of IBM Viruses	293
Subject Index	295