Malicious Cryptography

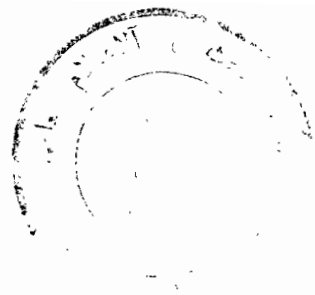
Exposing Cryptovirology

Adam Young

Moti Yung

WILEY

Wiley Publishing, Inc.



Dedicated to Elisa (A. Y.)
and to Maya (M. Y.)

Contents

Foreword xiii

Acknowledgments xix

Introduction xxi

1 Through Hacker's Eyes 1

2 Cryptovirology 33

3 Tools for Security and Insecurity 51
- 3.1 Sources of Entropy 53
- 3.2 Entropy Extraction via Hashing 54
- 3.3 Unbiasing a Biased Coin 57
  - 3.3.1 Von Neumann's Coin Flipping Algorithm 57
  - 3.3.2 Iterating Neumann's Algorithm 59
  - 3.3.3 Heuristic Bias Matching 60
- 3.4 Combining Weak Sources of Entropy 62
- 3.5 Pseudorandom Number Generators 66
  - 3.5.1 Heuristic Pseudorandom Number Generation 66
  - 3.5.2 PRNGs Based on Reduction Arguments 67
- 3.6 Uniform Sampling 68
- 3.7 Random Permutation Generation 71
  - 3.7.1 Shuffling Cards by Repeated Sampling 71
  - 3.7.2 Shuffling Cards Using Trotter-Johnson 73
- 3.8 Sound Approach to Random Number Generation and Use 76
- 3.9 RNGs Are the Beating Heart of System Security 77
- 3.10 Cryptovirology Benefits from General Advances 78
  - 3.10.1 Strong Crypto Yields Strong Cryptoviruses 78
  - 3.10.2 Mix Networks and Cryptovirus Extortion 80

7 Non-Zero Sum Games and Survivable Malware 147
7.1 Survivable Malware 148
7.2 Elements of Game Theory 150
7.3 Attacking a Brokerage Firm 151
7.3.1 Assumptions for the Attack 152
7.3.2 The Distributed Cryptoviral Attack 153
7.3.3 Security of the Attack 158
7.3.4 Utility of the Attack 159
7.4 Other Two-Player Game Attacks 161
7.4.1 Key Search via Facehuggers 161
7.4.2 Catalyzing Conflict Among Hosts 167
7.5 Future Possibilities 167

8 Coping with Malicious Software 171
8.1 Undecidability of Virus Detection 171
8.2 Virus Identification and Obfuscation 172
8.2.1 Virus String Matching 173
8.2.2 Polymorphic Viruses 176
8.3 Heuristic Virus Detection 182
8.3.1 Detecting Code Abnormalities 182
8.3.2 Detecting Abnormal Program Behavior 183
8.3.3 Detecting Cryptographic Code 191
8.4 Change Detection 197
8.4.1 Integrity Self-Checks 197
8.4.2 Program Inoculation 198
8.4.3 Kernel Based Signature Verification 199

9 The Nature of Trojan Horses 201
9.1 Text Editor Trojan Horse 202
9.2 Salami Slicing Attacks 202
9.3 Thompson's Password Snatcher 203
9.4 The Subtle Nature of Trojan Horses 206
9.4.1 Bugs May In Fact Be Trojans 208
9.4.2 RNG Biasing Trojan Horse 208

10 Subliminal Channels 211
10.1 Brief History of Subliminal Channels 212
10.2 The Difference Between a Subliminal and a Covert Channel 214
10.3 The Prisoner's Problem of Gustavus Simmons 215
10.4 Subliminal Channels New and Old 216

12.7.4 SETUP in the Schnorr Signature Algorithm 284
12.8 Rogue Use of DSA for Encryption 285
12.9 Other Work in Kleptography 286
12.10 Should You Trust Your Smart Card? 288

Appendix A: Computer Virus Basics **295**
A.1 Origins of Malicious Software 295
A.2 Trojans, Viruses, and Worms: What Is the Difference? . . 297
A.3 A Simple DOS COM Infector 299
A.4 Viruses Don't Have to Gain Control Before the Host . . . 303

Appendix B: Notation and Other Background Information **307**
B.1 Notation Used Throughout the Book 307
B.2 Basic Facts from Number Theory and Algorithmics 309
B.3 Intractability: Malware's Biggest Ally 312
B.3.1 The Factoring Problem 313
B.3.2 The e^{th} Roots Problem 314
B.3.3 The Composite Residuosity Problem 314
B.3.4 The Decision Composite Residuosity Problem . . . 315
B.3.5 The Quadratic Residuosity Problem 315
B.3.6 The Phi-Hiding Problem 315
B.3.7 The Phi-Sampling Problem 317
B.3.8 The Discrete Logarithm Problem 318
B.3.9 The Computational Diffie-Hellman Problem 318
B.3.10 The Decision Diffie-Hellman Problem 318
B.4 Random Oracles and Functions 319

Appendix C: Public Key Cryptography in a Nutshell **321**
C.1 Overview of Cryptography 321
C.1.1 Classical Cryptography 322
C.1.2 The Diffie-Hellman Key Exchange 324
C.1.3 Public Key Cryptography 325
C.1.4 Attacks on Cryptosystems 326
C.1.5 The Rabin Encryption Algorithm 330
C.1.6 The Rabin Signature Algorithm 331
C.1.7 The RSA Encryption Algorithm 332
C.1.8 The RSA Signature Algorithm 334
C.1.9 The Goldwasser-Micali Algorithm 335
C.1.10 Public Key Infrastructures 336
C.2 Discrete-Log Based Cryptosystems 337