a DEKKER series of TEXTBOOKS and MONOGRAPHS

Statistical Methods Computer Security

edited by
William W. S. Chen

Statistical Methods in Computer Security

edited by

William W. S. Chen
Internal Revenue Service
Washington, D.C., U.S.A.

15
SEMINAR LIBRARY
Department of Computer Science
UNIVERSITY OF KARACHI
25.4.09

Contents

Preface .... *iii*
Contributors .... *xi*

1. Development of Organizational Internet Security Policy: A Holistic Approach ***1***
Sharman Lichtenstein
1. Introduction 2
2. Organizational Internet Risks 5
3. Holistic Factors in Internet Security Policy 9
4. Framework for Developing Organizational Internet Security Policy 13
5. Internet Security Policy Content Model 16
6. Research Findings and Conclusion 16

2. Managing Software Security Risks: Buffer Overflows and Beyond ***23***
Gary McGraw
1. Software Security 23
2. Understanding the Problem 24
3. A Call to Arms 29

Experiments in Wireless Internet Security ... 33
Vipul Gupta and Sumit Gupta
Introduction 34
Secure Sockets Layer (SSL) 37
KSSL and KSecurity 40
Secure Mobile Enterprise Access 43
Technology Trends 44
6. Conclusions and Future Work 45

4. **The Neverending Saga of Internet Security: Why? How? and What to Do Next?** 49
Eddie Rabinovitch

5. **Secure Compartmented Data Access over an Untrusted Network Using a COTS-Based Architecture** 57
Paul C. Clark, Marion C. Meissner, and Karen O. Vance
1. Introduction 58
2. Security Architecture 60
3. Security Issues and Assumptions 64
4. Comparison with Related Work 66
5. Future Directions 68
6. Conclusion 69

6. **Internet Security** 71
Matt Bishop, Steven Cheung, Jeremy Frank, James Hoagland, Steven Samorodin, and Chris Wee
1. Introduction 71
2. Protection 74
3. Trust and Vulnerabilities 77
4. Audit 85
5. Intrusion Detection 88
6. Response 92
7. Assessment 93
8. Recovery 96
9. Conclusion: What of the F

7. **Computer Security: The Good, the Ba**
and the Ugly 101
Catherine Meadows
1. Introduction 102
2. Bad 103
3. Ugly 104
4. Good 105

8. **Architecture and Applications for a Distributed Embedded Firewall** *109*
Charles Payne and Tom Markham
1. Introduction 110
2. Objectives for EFW 112
3. Implementing EFW 118
4. Managing EFW 121
5. EFW Applications 123
6. Future Work 127
7. Summary 127

9. **Using Operating System Wrappers to Increase the Resiliency of Commercial Firewalls** *131*
Jeremy Epstein, Linda Thomas, and Eric Monteith
1. Introduction 132
2. Motivation 133
3. Wrappers Synopsis 134
4. Gauntlet Wrappers Using NAI Labs Wrappers 138
5. Wrapping Nonsource Firewalls Using NAI
Labs Wrappers 146
6. Wrapping Gauntlet Using ISI Wrappers 151
7. Current Status and Future Directions 153
8. Conclusion 155

10. **A Susceptible-Infected-Susceptible Model with Reintroduction for Computer Virus Epidemics** *157*
John C. Wierman
1. Introduction 158
2. The SIS Model 159

4. Analysis and Results 162
5. Discussion 165

11. Man vs. Machine—A Study of the Ability of Statistical Methodologies to Discern Human Generated ssh Traffic from Machine Generated scp Traffic 169
J.L. Solka, M.L. Adams, and E.J. Wegman
1. Introduction 170
2. Background 171
3. Results 172
4. Conclusions 179

12. Passive Detection of Denial of Service Attacks on the Internet 183
David J. Marchette
1. Introduction 183
2. Analysis 186
3. Experimental Results 189
4. Conclusions 209

13. On the Extinction of the S-I-S Stochastic Logistic Epidemic 213
Richard J. Kryscio and Claude Lefevre
1. Introduction 214
2. On the Mean Time Until Extinction 216
3. On the Quasi-Stationary Distribution 220

14. Secure Introduction of One-way Functions 229
Dennis Volpano
1. Introduction 229
2. The Language and Semantics 233
3. The Type System 237
4. The Reduction 238
5. Application to Password Systems 244
6. Conclusion 247

15. **Policy-Based Authentication and Authorization** **249**
Jeff Hayes
1. Overview 249
2. Authentication 250
3. Authorization 254
4. Policy Management 259
5. Policy Security 261
6. Conclusion 262

16. **The Evolution of Viruses and Worms** **265**
Thomas M. Chen and Jean-Marc Robert
1. Introduction 266
2. First Wave: Early Viruses and Worms 268
3. Second Wave: Polymorphism and Toolkits 270
4. Third Wave: Mass E-Mailers 271
5. Fourth Wave: Modern Worms 274
6. Current Developments 279
7. Conclusions 282

17. **Infrastructure Web: Distributed Monitoring and Managing Critical Infrastructures** **287**
Guofei Jiang, George Cybenko, and Dennis McGrath
1. Introduction 288
2. The Infrastructure Protection Process 290
3. Architecture 297
4. Related Work 305
5. Summary 306

18. **Firewalls: An Expert Roundtable** **309**
James P. Anderson, Sheila Brand, Li Gong, and Thomas Haigh
1. What are Firewalls? 310

19. **A New Model for Probabilistic Information Retrieval on the Web** **327**
Gabriel Mateescu, Masha Sosonkina, and Paul Thompson
1. Introduction 328

15. Policy-Based Authentication and Authorization ....

Jeff Hayes

1. Overview 249
2. Authentication 250
3. Authorization 254
4. Policy Management 259
5. Policy Security 261
6. Conclusion 262

16. The Evolution of Viruses and Worms **265**

Thomas M. Chen and Jean-Marc Robert

1. Introduction 266
2. First Wave: Early Viruses and Worms 268
3. Second Wave: Polymorphism and Toolkits 270
4. Third Wave: Mass E-Mailers 271
5. Fourth Wave: Modern Worms 274
6. Current Developments 279
7. Conclusions 282

17. Infrastructure Web: Distributed Monitoring and Managing Critical Infrastructures **287**

Guofei Jiang, George Cybenko, and Dennis McGrath

1. Introduction 288
2. The Infrastructure Protection Process 290
3. Architecture 297
4. Related Work 305
5. Summary 306

18. Firewalls: An Expert Roundtable **309**

James P. Anderson, Sheila Brand, Li Gong, and Thomas Haigh

1. What are Firewalls? 310

19. A New Model for Probabilistic Information Retrieval on the Web **327**

Gabriel Mateesеu, Masha Sosonkina, and Paul Thompson

1. Introduction 328

2. Background 329
3. Related Research 330
4. The Combination of Expert Opinion Model 331
5. Relevance Feedback 333
6. Probability Distributions in the Combination of Expert Opinion 334
7. Computing the Mean and Standard Deviation of the Transformed Beta Distribution 335
8. Discussion 338
9. Conclusion 340