Statistical Methods Computer Security

edited by William W. S. Chen

Statistical Methods in Computer Security

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

STMINAR LIBRARY

DEPARTMENT OF COMMENTS SCIENCE

UNIVERSITY OF CARROW

2.5-4-09

Contents

Preface iii	
Contributors xi	
1. Development of Organizational Internet	
Security Policy: A Holistic Approach	
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 County Policy Contest M. L.	
6. Research Findings and Conclusion 16	
2. Managing Software Security Risks; Buffer	
Overflows and Beyond	20
Gary McGraw	26
1. Software Security 23	
2. Understanding the Problem 24	
3. A Call to Arms 30	

	Contents
Experiments in Wireless Internet Security .	32
vipui Gupia ana Sumii Gupia	
Introduction 34	
Secure Sockets Layer (SSL) 37	
KSSL and KSecurity 40	
Secure Mobile Enterprise Access 43	
Technology Trends 44	
Conclusions and Future Work 45	
Concidental and Puttire Work 45	
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
6. Internet Security	
Matt Bishop, Steven Cheung, Jeremy Frank, Jame	8
Hoagland, Steven Samorodin, and Chris Wee 1. Introduction 71	
2. Protection 74	
3. Trust and Vulnerabilities 77	
A Andit OF	
5. Intrusion Detection 88	
6. Response 92	
7. Assessment 93	
8. Recovery 96	

a

Computer Security: The Good, the Daniel Computer Security: The Good Security: The Goo	
Security: The Go	
Computer Sec	
and the	
and the Ugo Catherine Meadows Introduction 102	
1. Introduced 103 2. Bad · · · · 104	
104	
3. 080, 100	
a Architecture and Applications for a	109
8. Architecture and Applications for a 8. Architecture Embedded Firewall	
8. Architecture and Application of the Property of the Propert	
ot lee Payne and I on	
a . Justian A.v	
Other thomas for P.P.W.	
a I-plementing EFW	
A Managing K.F.W	
4. Managing EFW 121 5. EFW Applications 123	
5. EFW Applications 125 6. Future Work 127	
6. Future Work	
7. Summary 127	
9. Using Operating System Wrappers to Increase	101
the Resiliency of Commercial Firewalls	131
Jeremy Epstein, Linda Thomas, and Eric Monteith	
1 Introduction 132	
2. Motivation 133	
3. Wrappers Synopsis 134	
4. Countlet Wronners Using NALLahr Wronners	100
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 159	
8. Conclusion 155	
10 4 0	
10. A Susceptible-Infected-Susceptible Model	
and a some outerion for Comment	
- Spidenics	
John C. Wierman	157
1. Introduction 150	
2. The SIS Model 150	
0 0	

****	Conten
4. Analysis and Results 162	
5. Discussion 165	
11. Man vs. Machine—A Study of the Ability Statistical Methodologies to Discern Hun Generated ssh Traffic from Machine Gene scp Traffic	nan
J.L. Solka, M.L. Adams, and E.J. Wegman	169
1. Introduction 170	
2. Background 171	
3. Results 172	
4. Conclusions 179	
12. Passive Detection of Denial of Service A	ttacks
on the Internet	183
David J. Marchette	Dinter S.
1. Introduction 183	
2. Analysis 186	
3. Experimental Results 189	
4. Conclusions 209	
13. On the Extinction of the S-I-S Stochastic	and on the last
Logistic Epidemic	
Richard J. Kryscio and Claude Lefevre	-
1. Introduction 214	
2. On the Mean Time Until Extinction 2	16
3. On the Quasi-Stationary Distribution	
5. On the Quasi-Stationary Distribution	
14. Secure Introduction of	
One-way Functions	
Dennis Volpano	
1. Introduction 229	
2. The Language and Semantics 233	
3. The Type System 237	
4. The Reduction 238	O SIB HAT
5. Application to Password Systems 244	To the state of the
C Construies 947	

949
and
Contents 15. Policy-Based Authentication and Authorization
pased Author
15. Policy-Dation
Authorization
Jeff Hayes 249
Quartiew . Zan
A AUTHORITY
A AUTURN - AUTURN
Dalicy areas
e Policy Section 262
5. Policy Security 6. Conclusion
16. The Evolution of Jean-Marc Robers
Thomas off
1. Introduction
o First Wave, Daily
1. Introduction 200 2. First Wave: Early Viruses and Worms
A Third Wave: Mass E-Mailers
4. Third Wave: Mass E-Maliers
5. Fourth Wave: Modern Works 6. Current Developments 279
7. Conclusions 282
7. Conclusions
17. Infrastructure Web: Distributed Monitoring
- 1 Managing Critical Infrastructures
Guofei Jiang, George Cybenko, and Dennis McGrath
Guofet diang, George Cyclina,
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 Sheile Pour 1 1: 5
James P. Anderson, Sheila Brand, Li Gong, and Thomas Haigh
The state of the s
1. What are Firewalls? 310
19. A New Model for Probabilistic Information Retrieval on the Web
Retrieval on the Web
Gabriel Mateesey Mark a
Paul Thomas Susonking and
1. Introduction
328

Contents 15. Policy-Based Authentication and Authorization	
teation	
thentics	
Contents assed Aut	
policy-Bation .	
15. Authoriza	
Leff Hayes 245 250	
wieW : 254 -0	
15. Authorized 249 Jeff Hayes 250 1. Overview 254 Authentication 254 Authentication 254	265
1. Overview 254 2. Authorization 254 2. Authorization 261	. 200
1. Overview 254 2. Authentication 254 2. Authorization 261 3. Authorization 261 4. Policy Management 262 5. Policy Security 262 5. Conclusion 262 6. Viruses and Worms 7. Conclusion 262	265
5 1 Lucion Dobelt	
3. Auto-Manage 4. Policy Security 5. Policy Security 6. Conclusion 6. Conclusion 7. Co	268
The Evolution and seasons	200 270
16. The Evolution 266 Thomas M. Chen and 266 1. Introduction Viruses and Worms 1. Introduction Early Viruses and Toolkits 1. First Wave: Early Viruses and Toolkits 271 2. First Wave: Polymorphism and 271 3. Second Wave: Mass E-Mailers 274 4. Third Wave: Mass E-Mailers 279	
troduction Viruses and Toolkie	
1. Introduce: Early Palymorphism 271	
2. First Wave: Poly E-Mailers	
1. Introduction Viruses 271 2. First Wave: Early Viruses 271 2. First Wave: Polymorphism and 271 3. Second Wave: Polymorphism and 271 4. Third Wave: Mass E-Mailers 274 4. Third Wave: Modern Worms 279 5. Fourth Wave: Modern 282	
4. Third Wave: Modern 279	
5. Fourth Developments	
4. Third Wave: Mass. 4. Third Wave: Modern Worms 5. Fourth Wave: Modern Worms 6. Current Developments 7. Conclusions 7. Conclu	nitoring 997
	-oc Zo.
17. Infrastructure Web: Distribute 17. Infrastructure 17. Infrastructure 17. Infrastructure Web: Distribute 17. Infrastructure 17. Infrastructure Web: Distribute 17. Infrastructure 1	McGrath
17. Infrastructing Critical Intra and Del	nnis McC.
Guofei Jiang, George 288	290
Guofei Jiang, George 238 1. Introduction 288 2. The Infrastructure Protection Process	
The Infrastructure Protection	
2. The Infrastructure 297 3. Architecture 305	
3. Architecture 305	
3. Architecture 305 4. Related Work 306	
4. Related Work 5. Summary 306	309
- Jan 10	
5. Summary	Gong, and Thomas
James P. Anderson, Shella Brand, De	
Haigh 1. What are Firewalls? 310	
1. What are Firewalls:	
	ation
19. A New Model for Probabilistic In	normation
Retrieval on the Web	327
Gabriel Mateeseu, Masha Sosonkino	i, and
Paul Thompson	
1. Introduction 328	

2. Background 329	
3. Related Research 330	
4. The Combination of Expert Opinion Model 3:	31
5. Relevance Feedback 333	
6. Probability Distributions in the Combination of	
Expert Opinion 334 Computing the Mean and Standard Deviation of	
the Transformed Beta Distribution 335	
the Transformed Beta 2	
B. Discussion 338	
O. Conclusion 340	