Secrets and Lies

DIGITAL SECURITY IN A NETWORKED WORLD

Bruce Schneier

WILEY

Wiley Publishing, Inc.

Contents

INTRODUCTION TO THE PAPERBACK EDITION xi

PREFACE xxi

1. INTRODUCTION 1

PART 1: THE LANDSCAPE 11

2. DIGITAL THREATS 14

3. ATTACKS 23

4. ADVERSARIES 42

5. SECURITY NEEDS 59

PART 2: TECHNOLOGIES 83

6. CRYPTOGRAPHY 85

7. CRYPTOGRAPHY IN CONTEXT 102

8. COMPUTER SECURITY 120

9. IDENTIFICATION AND AUTHENTICATION 135

10. NETWORKED-COMPUTER SECURITY 151

11. NETWORK SECURITY 176

12. NETWORK DEFENSES 188

13. SOFTWARE RELIABILITY 202

14. SECURE HARDWARE 212

15. CERTIFICATES AND CREDENTIALS 225

16. SECURITY TRICKS 240

17. THE HUMAN FACTOR 255

PART 3: STRATEGIES 271

18. VULNERABILITIES AND THE VULNERABILITY LANDSCAPE 274

19. THREAT MODELING AND RISK ASSESSMENT 288

20. SECURITY POLICIES AND COUNTERMEASURES 307

21. ATTACK TREES 318

22. PRODUCT TESTING AND VERIFICATION 334

23. THE FUTURE OF PRODUCTS 353

24. SECURITY PROCESSES 367

25. CONCLUSION 389

AFTERWORD 396

RESOURCES 399

ACKNOWLEDGMENTS 401

INDEX 403