Contents

Foreword xxvii

Chapter 1 The Wireless Challenge 1

Introduction 2
Wireless Technology Overview 2
Defining Cellular-based Wireless 3
Defining the Wireless LAN 3
The Convergence of Wireless Technologies 3
Trends and Statistics 4
Increasing Use of Information Appliances 5
The Future of Wireless, circa 2005 6
Understanding the Promise of Wireless 7
Wireless Networking 9
Wireless Networking Applications for Business 9
Wireless Networking Applications for Consumers 14
Understanding the Benefits of Wireless 16
Convenience 16
Flexibility 16
Roaming 18
Mobility 21
Affordability 22
Speed 22
Aesthetics 24
Productivity 24
Facing the Reality of Wireless Today 24
Standards Conflicts 25
Commercial Conflicts 27
Market Adoption Challenges 27
The Limitations of "Radio" 27
Radio Range and Coverage 30
Use of Antennas 30
Interference and Coexistence 31

Answers to Your Wireless Questions

Q: Will i-Mode be available in North America or Europe?

A: Although i-Mode parent NTT DoCoMo has ownership stakes in several North American and European cellular operators, it is not expected that i-Mode, as it currently exists, will be offered in these markets. This is primarily due to the limited 9.6 Kbps access rates.

The Limitations of Wireless Security 32
Cellular-based Wireless Networks and WAP 34
Wireless LAN Networks and WEP 35
Examining the Wireless Standards 38
Cellular-based Wireless Networks 38
Communications Technologies 39
Wireless LAN Networks 46
802.11 WLAN 47
HomeRF 54
802.15 WPAN 57
802.16 WMAN 60
Understanding Public Key Infrastructures and Wireless Networking 62
Overview of Cryptography 63
Summary 68
Solutions Fast Track 69
Frequently Asked Questions 73

Chapter 2 A Security Primer 75
Introduction 76
Understanding Security Fundamentals and Principles of Protection 76
Ensuring Confidentiality 77
Ensuring Integrity 78
Ensuring Availability 80
Ensuring Privacy 81
Ensuring Authentication 81
Ensuring Authorization 85
Ensuring Non-repudiation 87
Accounting and Audit Trails 90
Using Encryption 92
Encrypting Voice Data 92
Encrypting Data Systems 93
Reviewing the Role of Policy 93
Identifying Resources 96
Understanding Classification Criteria 97

Implementing Policy 98
Recognizing Accepted Security and Privacy Standards 101
Reviewing Security Standards 101
Early Security Standards 102
Understanding the Common Criteria Model 104
ISO 17799/BS 7799 104
ISO 7498-2 104
ISO 10164-8 104
ISO 13888 105
Reviewing Privacy Standards and Regulations 106
NAIC Model Act 106
Gramm-Leach-Bliley Act 106
HIPAA 108
Electronic Signatures in the Global and National Commerce Act 111
COPPA 112
Civil Liability Law 112
Addressing Common Risks and Threats 113
Experiencing Loss of Data 113
Loss of Data Scenario 113
Experiencing Denial and Disruption of Service 114
Disruption of Service Scenario 114
Eavesdropping 115
Eavesdropping Scenario 117
Preempting the Consequences of an Organization's Loss 117
Security Breach Scenario 118
Summary 119
Solutions Fast Track 120
Frequently Asked Questions 123

Tools & Traps…

Clear-text Authentication

An example of a brute-force password dictionary generator that can produce a brute-force dictionary from specific character sets can be found at www.dmzs.com/tools/files. Other brute force crackers, including POP, Telnet, FTP, Web and others, can be found at http://packetstormsecurity.com/crackers.

Chapter 3 Wireless Network Architecture and Design 125

Introduction 126
Fixed Wireless Technologies 127
Multichannel Multipoint Distribution Service 127
Local Multipoint Distribution Services 129
Wireless Local Loop 129
Point-to-Point Microwave 130
Wireless Local Area Networks 132
Why the Need for a Wireless LAN Standard? 132
What Exactly Does the 802.11 Standard Define? 134
Does the 802.11 Standard Guarantee Compatibility across Different Vendors? 137
802.11b 138
802.11a 139
802.11e 140
Developing WLANs through the 802.11 Architecture 141
The Basic Service Set 141
The Extended Service Set 143
Services to the 802.11 Architecture 143
The CSMA-CA Mechanism 145
The RTS/CTS Mechanism 146
Acknowledging the Data 146
Configuring Fragmentation 147
Using Power Management Options 147
Multicell Roaming 147
Security in the WLAN 148
Developing WPANs through the 802.15 Architecture 150
Bluetooth 150
HomeRF 153
High Performance Radio LAN 153
Mobile Wireless Technologies 154
First Generation Technologies 155

Fixed Wireless Technologies

In a fixed wireless network, both transmitter and receiver are at fixed locations, as opposed to mobile. The network uses utility power (AC). It can be point-to-point or point-to-multipoint, and may use licensed or unlicensed spectrums.

Second Generation Technologies 156
2.5G Technology 156
Third Generation Technologies 156
Wireless Application Protocol 157
Global System for Mobile Communications 158
General Packet Radio Service 160
Short Message Service 160
Optical Wireless Technologies 160
Exploring the Design Process 161
Conducting the Preliminary Investigation 162
Performing Analysis of the Existing Environment 162
Creating a Preliminary Design 163
Finalizing the Detailed Design 164
Executing the Implementation 164
Capturing the Documentation 165
Creating the Design Methodology 166
Creating the Network Plan 166
Gathering the Requirements 167
Baselining the Existing Network 168
Analyzing the Competitive Practices 169
Beginning the Operations Planning 169
Performing a Gap Analysis 169
Creating a Technology Plan 170
Creating an Integration Plan 171
Beginning the Collocation Planning 171
Performing a Risk Analysis 171
Creating an Action Plan 172
Preparing the Planning Deliverables 172
Developing the Network Architecture 173
Reviewing and Validating the Planning Phase 173
Creating a High-Level Topology 173
Creating a Collocation Architecture 174
Defining the High-Level Services 174
Creating a High-Level Physical Design 175

Defining the Operations Services 175
Creating a High-Level Operating Model 175
Evaluating the Products 176
Creating an Action Plan 177
Creating the Network Architecture Deliverable 177
Formalizing the Detailed Design Phase 177
Reviewing and Validating the Network Architecture 178
Creating the Detailed Topology 178
Creating a Detailed Service Collocation Design 179
Creating the Detailed Services 179
Creating a Detailed Physical Design 180
Creating a Detailed Operations Design 181
Creating a Detailed Operating Model Design 181
Creating a Training Plan 182
Developing a Maintenance Plan 182
Developing an Implementation Plan 182
Creating the Detailed Design Documents 183
Understanding Wireless Network Attributes from a Design Perspective 183
Application Support 184
Subscriber Relationships 186
Physical Landscape 187
Network Topology 189
Summary 191
Solutions Fast Track 193
Frequently Asked Questions 198

Chapter 4 Common Attacks and Vulnerabilities 201
Introduction 202
The Weaknesses in WEP 202
Criticisms of the Overall Design 203
Weaknesses in the Encryption Algorithm 205

Weaknesses in Key Management 208
Weaknesses in User Behavior 211
Conducting Reconnaissance 213
Finding a Target 213
Finding Weaknesses in a Target 214
Exploiting Those Weaknesses 215
Sniffing, Interception, and Eavesdropping 216
Defining Sniffing 216
Sample Sniffing Tools 217
Sniffing Case Scenario 217
Protecting Against Sniffing and Eavesdropping 219
Spoofing and Unauthorized Access 220
Defining Spoofing 220
Sample Spoofing Tools 221
Spoofing Case Scenario 221
Protecting Against Spoofing and Unauthorized Attacks 223
Network Hijacking and Modification 223
Defining Hijacking 223
Sample Hijacking Tools 224
Hijacking Case Scenario 225
Protection against Network Hijacking and Modification 225
Denial of Service and Flooding Attacks 226
Defining DoS and Flooding 226
Sample DoS Tools 227
DoS and Flooding Case Scenario 227
Protecting Against DoS and Flooding Attacks 228
The Introduction of Malware 228
Stealing User Devices 230
Summary 232
Solutions Fast Track 232
Frequently Asked Questions 237

Notes from the Underground…

Lucent Gateways broadcast SSID in clear on encrypted networks

It has been announced (www.securiteam.com/securitynews/5ZP0I154UG.html) that the Lucent Gateway allows an attacker an easy way to join a closed network.

Lucent has defined an option to configure the wireless network as "closed." This option requires that to associate with the wireless network a client must know and present the SSID of the network. Even if the network is protected by WEP, part of the broadcast messages the gateway transmits in cleartext includes the SSID. All an attacker need do is sniff the network to acquire the SSID, they are then able to associate with the network.

Chapter 5 Wireless Security Countermeasures 239

Introduction 240
Revisiting Policy 241
Addressing the Issues with Policy 243
Analyzing the Threat 245
Threat Equals Risk Plus Vulnerability 246
Designing and Deploying a Secure Network 253
Implementing WEP 257
Defining WEP 257
Creating Privacy with WEP 258
The WEP Authentication Process 259
WEP Benefits and Advantages 259
WEP Disadvantages 260
The Security Implications of Using WEP 260
Implementing WEP on the Aironet 261
Implementing WEP on the ORiNOCO AP-1000 262
Securing a WLAN with WEP: A Case Scenario 262
Filtering MACs 264
Defining MAC Filtering 265
MAC Benefits and Advantages 266
MAC Disadvantages 266
Security Implications of MAC Filtering 267
Implementing MAC Filters on the AP-1000 267
Implementing MAC Filters on the Aironet 340 269
Filtering MAC Addresses: A Case Scenario 270
Filtering Protocols 271
Defining Protocol Filters 271
Protocol Filter Benefits and Advantages 272
Protocol Filter Disadvantages 272
Security Implications of Using Protocol Filters 272
Using Closed Systems and Networks 273
Defining a Closed System 273

Guidelines for Analyzing Threats

- Identify assets
- Identify the method of accessing these valuables from an authorized perspective
- Identify the likelihood that someone other than an authorized user can access valuables
- Identify potential damages
- Identify the cost to replace, fix, or track the loss
- Identify security countermeasures
- Identify the cost in implementation of the countermeasures
- Compare costs of securing the resource versus cost of damage control

Closed System Benefits and Advantages 274
Closed System Disadvantages 275
Security Implications of Using a Closed System 275
A Closed Environment on a Cisco Aironet Series AP 275
A Closed Environment on an ORiNOCO AP-1000 275
Implementing a Closed System: A Case Scenario 277
Enabling WEP on the ORiNOCO Client 277
Allotting IPs 278
Defining IP Allocation on the WLAN 278
Deploying IP over the WLAN: Benefits and Advantages 279
Deploying IP over the WLAN: Disadvantages 279
Security Implications of Deploying IP over the WLAN 280
Deploying IP over the WLAN: A Case Scenario 280
Using VPNs 281
VPN Benefits and Advantages 283
VPN Disadvantages 284
Security Implications of Using a VPN 284
Layering Your Protection Using a VPN 285
Utilizing a VPN: A Case Scenario 286
Securing Users 287
End User Security Benefits and Advantages 290
End User Security Disadvantages 290
User Security: A Case Scenario 291
Summary 292
Solutions Fast Track 293
Frequently Asked Questions 296

Chapter 6 Circumventing Security Measures 299

Introduction 300
Planning and Preparations 300
Finding a Target 301
Choosing the Tools and Equipment Required for Attack 301
Detecting an Open System 302
Detecting a Closed System 303
Exploiting WEP 303
Security of 64-bit versus 128-bit Keys 304
Acquiring a WEP Key 305
War Driving 306
What Threat Do These "Open Networks" Pose to Network Security? 307
What Tools Are Necessary to Perform a War Drive? 307
What Network Information Can I Discover from a War Drive? 308
Can War Driving Be Detected? 310
Stealing User Devices 310
What Are the Benefits of Device Theft? 311
MAC Filtering 312
What Is a MAC Address? 312
Where in the Authentication/Association Process Does MAC Filtering Occur? 313
Determining MAC Filtering Is Enabled 314
MAC Spoofing 314
Bypassing Advanced Security Mechanisms 315
Firewalls 316
Filtering by IP Address 316
Filtering by Port 317
What Happens Now? 317
Exploiting Insiders 318
What Is at Stake? 318
Social Engineering Targets 319

War Driving

War driving has become the common term given for people who drive around with wireless equipment looking for other wireless networks. This term gets its history from "war-dialing" – the age old practice of having your computer dial every phone number within a certain range to see if a computer would pick up.

Installing Rogue Access Points 320
Where Is the Best Location for a Rogue AP? 320
Configuring the Rogue AP 321
Risks Created by a Rogue AP 321
Are Rogue APs Detectable? 321
Exploiting VPNs 322
Summary 323
Solutions Fast Track 323
Frequently Asked Questions 326

Chapter 7 Monitoring and Intrusion Detection 327

Introduction 328
Designing for Detection 328
Starting with a Closed Network 329
Ruling Out Environmental Obstacles 330
Ruling Out Interference 331
Defensive Monitoring Considerations 331
Availability and Connectivity 332
Interference and Noise 332
Signal Strength 333
Detecting a Denial of Service 334
Monitoring for Performance 335
Knowing the Baseline 335
Monitoring Tools of the Trade 336
Intrusion Detection Strategies 337
Integrated Security Monitoring 338
Watching for Unauthorized Traffic and Protocols 339
Unauthorized MAC Addresses 341
Popular Monitoring Products 342
Signatures 343
Conducting Vulnerability Assessments 346
Incident Response and Handling 348
Policies and Procedures 350
Reactive Measures 350

Defensive Monitoring Considerations

- Define your wireless network boundaries, and monitor to know if they're being exceeded
- Limit signal strength to contain your network.
- Make a list of all authorized wireless Access Points (APs) in your environment. Knowing what is supposed to be there can help you immediately identify rogue APs.

Reporting 351
Cleanup 352
Prevention 352
Conducting Site Surveys for Rogue Access Points 353
The Rogue Placement 353
The Well-intentioned Employee 353
The Social Engineer 354
Tracking Rogue Access Points 355
Summary 358
Solutions Fast Track 359
Frequently Asked Questions 361

Chapter 8 Auditing 363
Introduction 364
Designing and Planning a Successful Audit 364
Types of Audits 365
Assessing Risk 365
Measuring System Operation 367
Measuring System Compliance 368
Verify Change Management 368
Assessing Damage 368
When to Perform an Audit 369
At System Launch 370
On Schedule 370
Maintenance Window 370
Unplanned Emergency Audits 371
Auditing Activities 371
Audit Planning 372
Audit Information Gathering 372
Audit Information Analysis and Report Generation 372
Audit Report Presentation 373
Post-audit Review 373
Next Steps 373
Auditing Tools 374
Auditing Interview Tools 374

Auditing Activities

Wireless network audits consist of several stages where different resources or tools are needed to perform a specific activity. These activities generally fall into six categories:

- Audit Planning
- Audit Information Gathering
- Audit Information Analysis and Report Generation
- Audit Report Presentation
- Post-Audit Review
- Next Steps

Technical Auditing Tools 375
Critical Auditing Success Factors 376
Defining Standards 377
Standards 378
Guidelines 378
Best Practices 378
Policies 378
Procedures 379
Auditing, Security Standards, and Best Practices 379
Corporate Security Policies 382
Auditing Charters and Irregularities 384
Sampling Irregularities 384
Biased Opinions 384
Fraud 385
Establishing the Audit Scope 385
Establishing the Documentation Process 386
Performing the Audit 386
Auditors and Technologists 386
Obtaining Support from IS/IT Departments 387
Senior Management Support 387
IS/IT Department Support 388
Gathering Data 388
Interviews 389
Document Review 389
Technical Review 390
Analyzing Audit Data 390
Matrix Analysis 391
Recommendations Reports 392
Generating Audit Reports 392
The Importance of Audit Report Quality 393
Writing the Audit Report 393
Executive Summary 394
Prioritized Recommendations 394
Main Body 394
Detailed Recommendations 395
Final Conclusions 396

Implementing an Ultra Secure WLAN

- Make sure that your AP allows you to change ESSID, passwords and supports 128-bit WEP.
- Find an AP that supports the "closed network" functionality.
- Be certain that the AP you buy supports flash upgrades.
- Isolate the AP and regulate access from its network into your internal network.
- Conduct audits of your network using NetStumbler or other wireless scanning tools to make sure that others aren't enabling unauthorized APs.
- Update security policy to reflect the dangers of an unsecured wireless network.

Appendices 396
Glossary 396
Final Thoughts on Auditing 396
Sample Audit Reports 397
Sample Management Report: Wireless Network Security Audit Report XYZ Corporation 397
Sample Technical Report Wireless Network Security Audit Report: XYZ Corporation 398
Summary 402
Solutions Fast Track 403
Frequently Asked Questions 406

Chapter 9 Case Scenarios 407
Introduction 408
Implementing a Non-secure Wireless Network 409
Implementing an Ultra-secure Wireless LAN 410
Physical Location and Access 411
Configuring the AP 412
Designing Securely 413
Securing by Policy 417
Taking a War Drive 418
Scouting Your Location 426
Installing in Difficult Situations 427
Developing a Wireless Security Checklist 429
Minimum Security 429
Moderate Security 430
Optimal Security 431
Summary 433
Solutions Fast Track 434
Frequently Asked Questions 436

Appendix: Hack Proofing Your Wireless Network Fast Track 439

Index 467