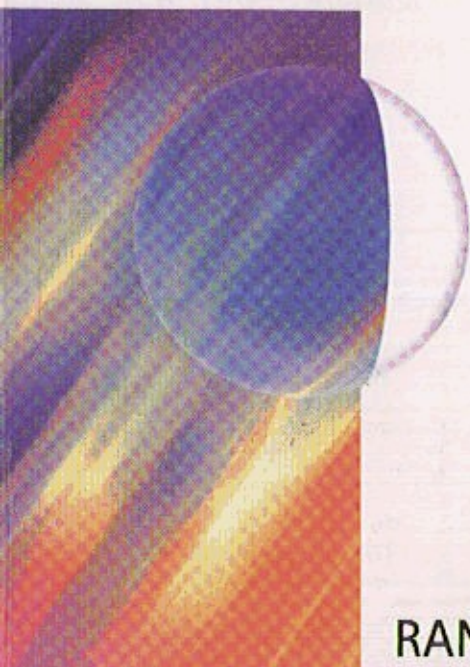


McGraw-Hill TELECOM

PROFESSIONAL

WIRELESS SECURITY

Models, Threats, and Solutions



Learn to recognize the threats and vulnerabilities unique to wireless communications

Plan application-aware cryptographic defenses and review available solutions

Specify defenses for telecom, broadband, satellite, and other markets soon to come

RANDALL K. NICHOLS • PANOS C. LEKKAS

INTERNATIONAL EDITION

Contents

Foreword *xxi*

Preface *xxv*

List of Contributors *xxxiii*

1 Why is Wireless Different? *1*

Introduction	<i>1</i>
Protecting the Means Of Communication	<i>2</i>
Protecting Privacy	<i>2</i>
Promoting Safety	<i>4</i>
The Personal and the Public	<i>5</i>
Shaking Up the Status Quo	<i>6</i>
Understanding Wireless Forecasts	<i>7</i>
Reasonable Degrees of Security	<i>8</i>
Regulatory Environments and Issues	<i>9</i>
Security-Related Regulations	<i>9</i>
Security-Related Market Factors	<i>10</i>
Guidelines for Security Measures	<i>10</i>
Cellular Networks and Bearer Technologies	<i>12</i>
First-Generation Wireless (1G)	<i>16</i>
Second-Generation Wireless (2G)	<i>16</i>
Spread Spectrum	<i>19</i>
Code Division Multiple Access (CDMA)	<i>20</i>
Time Division Multiple Sccess (TDMA)	<i>21</i>
Global System for Mobile Communications (GSM)	<i>22</i>
Third-Generation Wireless (3G)	<i>24</i>
Short Message Service (SMS)	<i>24</i>
Fourth-Generation Wireless (4G)	<i>27</i>
Summary	<i>28</i>
Endnotes	<i>28</i>

2	Wireless Information Warfare	37
	Wireless Is Information Warfare (IW)	37
	A Functional Taxonomy Based on Information Warfare	38
	Taxonomies of Wireless Communications Networks	43
	A Classification Scheme Based on Network Architecture	44
	Wireless Systems With a Fixed Supporting Infrastructure	44
	Wireless Systems in Which Users Communicate Directly	
	Through a Satellite or Satellites	45
	Wireless Data Networks That Are Fully Mobile	45
	Wireless Systems with No Supporting Infrastructure Other	
	Than the Mobile Nodes Themselves	45
	A Taxonomy Based on Mobility Only	46
	Tethered Mobility with Fixed Base Stations	47
	Fully Mobile Networks ("Comm on The Move")	47
	Circuit-Switched Networks and Packet-Switched Networks	48
	Information Theory	49
	Entropy	49
	Mobile Capacity	52
	Spectral Efficiency	53
	Decision Theory	56
	Risk Management and Architecture of Information Security	
	(INFOSEC)	57
	Thinking About Risk	57
	Vulnerability	58
	Threats	58
	Countermeasures	59
	Impact	59
	A Model for Cost-Effective Risk Management	60
	Historical Threats to Wireless Services OTA	62
	Why Is Wireless Security Different?	63
	Physical Layer Security	64
	Data Link and Network Layers	64
	Transport Layer Security	64
	Application Layer Security	65
	Performance Measures and Key Design Tradeoffs	66
	High-Level Performance Measures	67
	Low-Level Performance Measures	67
	Military-Unique System Requirements	68
	Offensive Information Operations	70
	A Taxonomy of Attack Operations	72
	Cryptographic Attacks	81
	Defensive Information Operations	84
	Cryptographic Measures	85
	Key Management	86
	Electromagnetic Capture Threats	88
	Summary	90
	Endnotes	90

3 Telephone System Vulnerabilities 93

- Interception/Ease of Interception 94
- Interruption of Service 95
- Unintentional Interruptions 95
- Natural Hazards 96
 - Hurricanes 96
 - Tornadoes 97
 - Winter storms 97
 - Flooding 97
 - Earthquakes 97
 - Fire 98
 - Power outages 98
 - Software failures 98
- Intentional Interruptions 98
 - Phone Phreaking 100
 - Legal Aspects 100
 - Laws in the United States 101
 - Privacy 101
 - Cryptography 101
 - Jamming 103
 - Right to Free Speech and Privacy Expectations When Using Cell Phones 103
 - Who Is Doing The Intercepting? 104
 - Joe Q. Public 105
 - Mobile Telephones 105
 - Cellular Telephones 105
 - Friends and Neighbors: The Unintentional Intercept 105
 - Voice Systems 106
 - Data Systems 106
 - Criminal Arena 107
 - Fraud 107
 - Pagers 108
 - Drugs Cartels 109
 - Military—United States 109
 - Other Countries 110
 - ECHELON 112
 - ECHELON Ground Stations 113
 - Future Research 113
 - Law Enforcement 115
 - Applications 116
- Cell Phone Vulnerabilities 117
 - Jamming 117
 - Interception 118
 - Countermeasures to Jamming and Interception 119
 - Code Division Multiple Access (CDMA) 120
 - Who's Listening to Cell Phone Conversations? 121

- Fraud 121
- Countermeasures to Fraud 121
- History of Cordless Telephones 122
- Handset Features 122
- Handset Vulnerabilities 123
- Countermeasures 124
- Microphones 125
- Types of Microphones 125
- Use of Microphones 127
- Countermeasures 128
- RF Data Communications 128
- Short Range: < 100 Feet 128
- Medium Range: 150 feet to 300 yards 129
- Issue of Privacy 129
- Summary 130
- Endnotes 130

4 Satellite Communications 133

- History 133
- Satellite Orbits 135
- Geostationary Orbit 135
- Highly Elliptical Orbit 136
- Low Earth Orbit/Medium Earth Orbit 137
- Navigation and Tracking 140
- Global Positioning System 140
- Wide Area Augmentation System 140
- Satellite Search and Rescue 140
- Communications: Voice, Video, and Data 141
 - Voice 141
 - Video, Audio, and Data 142
- Satellite Internet 143
- Earth Sensing: Commercial Imaging 143
- Landsat 144
- SPOT 144
- European Remote Sensing 144
- IKONOS 144
- Satellite Spectrum Issues 145
- Instruments and Goals of Current U.S. Satellite Encryption Policy 147
 - Issues Associated With Current U.S. Policy 147
- Federal Information Processing Standards 148
- International Policy Concerns 149
 - Export Controls On Satellite Encryption: U.S. Objectives 149
 - Licensing and the U.S. Munitions List (USML) 150
 - Impact of Export Controls 150
 - Are Export Controls Effective? 151
 - Legal Issues for Satellite Encryption: Privacy 151

- Computer crime 153
 - Surveillance 153
 - Patents 154
 - Public-Key Encryption for Satellite Communication 154
 - Escrowed Encryption for Satellite Communications 155
 - Impact on Information Security (INFOSEC) and Law Enforcement 155
- Importance to the U.S. of Space Exploitation and Control 156
 - Deterrence 156
- National and International Defense 156
- Surveillance 156
- Development, Implementation, and Management of Advanced Satellite Encryption Options and Strategies 157
 - Planning, Details, and Implementation 157
- Options for Serving Data Consumers 160
- Framework for Dealing With Policy Issues 160
 - Protection of Personal Data and Privacy 162
- Security of Information Systems 163
 - Intellectual Property Protection 167
 - Demand for Hardware-Based Data Security 169
- Balancing Information Technology, National Security, and Personal Privacy 170
 - State of the Revolution 170
 - The Pitfalls and the Potential 170
- Information Vulnerability 171
- Importance of Information 172
 - At Risk 173
 - Information Warfare 173
- Summary 173
- Endnotes 174

5 Cryptographic Security 177

- Concealment 177
- First Principles 179
- Lock-and-Key Analogy 180
- Transposition Ciphers 181
- Substitution Ciphers 182
- Kerckhoff's Principles 184
- Product Ciphers 184
- Classical Cryptanalysis 185
- Digital Cryptography 186
- Pseudo-Random Number Generation 190
- What Is Random? 191
- Pseudo-Random Number Generator (PRNG) 191
- The Seed and Entropy 192
- Seed as Key? 193

The One-Time Pad	194
The Data Encryption Standard	195
Avalanche Effect	197
A Standard Under Fire -DES Isn't Strong Anymore	197
Modern Cipher Breaking	198
Key Processing Rate	198
Brute Force Attacks	198
Standard Attacks	200
Advanced Attacks	202
Two Limits of Encryption	203
Block versus Stream Ciphers	204
Stream Cipher Design Considerations	205
The Stream Cipher Synchronization Problem	207
Non-Keyed Message Digests	208
SHA	209
SHA-1 in the Encryption Mode	209
HORNET™	210
Entropy Accumulator Description	212
Sync, Pad, and Data Encryption Key (DEK) Generation	214
Advanced Encryption Standard	217
Key Management-Generation and Distribution of Keys	219
Public-Key Systems-The Second Revolution	221
Public-Key Distribution and Diffie-Hellman	222
Digital Signatures	223
Certificate Authorities	224
Using Public-Key Cryptography for Key Management	225
Algorithms	226
Difficulty of Mathematical Systems	227
Integer Factorization Systems	228
Security	228
Implementation	229
Discrete Logarithm Systems	229
Security	229
Implementation	230
The Elliptic Curve Cryptosystem (ECC)	230
Security	232
Implementation	232
Comparison of Public-Key Cryptographic Systems	233
Efficiency	234
Computational overheads	235
Key Size Comparison	235
Bandwidth	235
ECDLP and Wireless Devices	235
Key Generation in Wireless Devices for IFP, DLP, and ECDLP	237
Bandwidth in Wireless Devices	237
Scalability	238

Processing Overhead	238
Smart cards	239
Cellular Phone Networks	241
Handheld Computers/Personal Digital Assistant (PDAs)	242
BSAFE Crypto-C	243
Cryptography in Embedded Hardware: FPGA and ASICs	243
FPGA Overview	245
FPGA-Based Cryptography	246
Results	247
Summary	247
Endnotes	249

6 Speech Cryptology 253

It Started with SIGSALY	253
Vetterlein's Forschungsstelle	254
Digitizing Voice Information via SIGSALY	256
Overview of SIGSALY Encryption Process for Single Vocoder Channel	261
Cryptology of Speech Signals	262
Speech: Production and Nonlinguistic Properties	262
The Structure of Language	263
Phonemes and Phones	264
Historical Linguistics	266
Threads	268
Writing Systems	268
Classic Source-Filter Model	268
General Source-Filter Model	270
Continuous Speech Spectrogram	271
Sampling of the Speech Waveform	275
The Fourier Transform	281
The Fast Fourier Transform (FFT)	283
Windowing Signal Segments	283
Window Function	284
Linear Prediction Modeling	286
Quantization and PCM	288
Transmission of Speech Signals	290
Synchronization	290
Cryptography of Speech Signals	292
Analog Scramblers	293
Frequency Inverters	294
Band Splitters	295
Two-Band-Splitter	295
Band-Shifter	295
Band-Inverter	295
Bandshift-Inverter	297
n-Band-Splitter	297

Transform Based Scramblers (TBSs)	300
Time Domain Scramblers (TDSs)	301
Time Element Scrambling	303
Hopping Window	304
Sliding Window	304
Two-Dimensional Scramblers	304
Digital Scramblers	307
Source Coding of Speech	309
Formant Vocoder	309
Channel Vocoder	309
Linear Prediction Based Vocoder (LP)	311
Reflection Coefficients	311
Log Area Ratio Coefficients	313
Sinusoidal Model	314
Sinusoidal Parameter Analysis	315
Standards	316
Cryptanalysis of Speech Systems	316
Tools and Parameters for Cryptanalysis of Speech	317
Application of Sound Spectrograph to Cryptanalysis	317
Analog Methods	321
Cryptanalysis of Digital Scramblers/Ciphers	322
Noise Cancellation	322
Cryptanalysis of Linear Prediction Based Vocoders	323
Thoughts About Cryptanalysis of Public-Key Systems	324
Cryptanalysis of A5 Algorithm	324
Summary	325
Endnotes	325
7 The Wireless Local Area Network (WLAN)	329
Wireless Transmission Media	330
Infrared Systems	331
Narrowband Radio Systems	331
Wideband Radio Systems: Spread Spectrum	331
Frequency-Hopping Spread Spectrum (FHSS)	332
Direct-Sequence Spread Spectrum (DSSS)	332
WLAN Products and Standards—Today's Leaders?	333
802.11 Security?	333
IEEE 802.11b	334
Securing WLANs	334
Eavesdropping	334
Unauthorized Access	335
Interference and Jamming	336
Physical Threats	336
Countermeasures	337
Frequency-Hopping Spread Spectrum (FHSS)	337
Direct-Sequence Spread Spectrum (DSSS)	337

- Infrared (IR) 340
- Narrowband 340
- The Infamous WEP 340
 - Encryption 340
 - Authentication 343
 - Wired Equivalency Protocol Flaws Too Public 344
 - Other Authentication Techniques 344
- Physical Security 344
- Summary 345
- Endnotes 345
- 8 Wireless Application Protocol(WAP) 349**
 - Comparison of the TCP/IP, OSI, and WAP Models 350
 - How WAP Works 352
 - The Security Status of WAP 354
 - Viruses 356
 - Authorization 357
 - Non-repudiation 357
 - Authentication 358
 - Secure Sessions 358
 - Security Products 358
 - Securant Technologies™ ClearTrust Control 362
 - WAP Security Architecture 362
 - Marginal Security 363
 - Wireless Access to the Internet 363
 - Wireless Middleware 363
 - Summary 364
 - Endnotes 364
- 9 Wireless Transport Layer Security (WTLS) 367**
 - Secure Socket Layer 367
 - Record Protocol 369
 - SSL Handshake Protocol 370
 - Transport Layer Security 371
 - Advantages and Disadvantages of SSL/TLS 371
 - Netscape 372
 - Microsoft 372
 - Entrust 372
 - EAP-TLS 372
 - Alternatives to SSL/TLS 374
 - IP Security (IPSec) 374
 - Authentication Header Protocol (AH) 375
 - Encapsulating Security Payload (ESP) 377
 - Transport and Tunnel Modes 377
 - Secure Shell (SSH) 378
 - SSH Transport Layer Protocol 378

SSH Versus TLS Implementations	380
Light Extensible Authentication Protocol (LEAP)	380
Wireless Transport Layer Security and WAP	381
Understanding Wireless Transport Layer Security	382
WTLS Handshake Protocol	382
WTLS Alert Protocol	383
WTLS Change Cipher Protocol	383
Pros and Cons of WTLS	384
WTLS Vulnerabilities	384
Implementations of WTLS	385
Additional Sources	386
Endnotes	387

10 Bluetooth 389

Bluetooth Basic Specifications	390
Bluetooth Technology	390
Bluetooth Specification Development	391
Design Decisions	392
Piconets	393
Bluetooth Security Architecture	394
Scatternets	396
The Bluetooth stack	397
Security Functions at the Baseband Layer	398
Security Functions of the Service Discovery Protocol	399
Security Functions at the Link Layer	400
Frequency-Hopping	401
Channel Establishment	401
Security Manager	402
Authentication	406
Authentication with the SAFER1 Block Cipher	408
Encryption	409
Encryption Modes	409
Key Length Negotiation	410
Encryption With the E0 Stream Cipher	410
Threats to Bluetooth Security	413
Jamming	413
Bluetooth holes	414
Summary and Security Assessment	415
Endnotes	416

11 Voice Over Internet Protocol 423

VoIP Generally Speaking	423
The Buzz Around VoIP	424
VoIP Standards	424
The Rise of VoIP Technology	427
Network Traffic	427
Billing and Interoperability Dilemma	428

Interoperability	428
Competitive Long Distance Rates	429
Caution: Implementation Ahead	429
The Vendor Market	429
Technical Issues for VoIP Calling	434
Speech Encoding	434
Voice Network Security Vulnerabilities	435
Confidentiality, Integrity, and Availability Attributes	435
VoIP and the Wireless Security Environment	436
Private Networks	436
WEP	436
Confidentiality, Integrity, and Availability in VoIP Implementations	436
IP Spoofing and VoIP	437
Interception and Eavesdropping of Voice Transmission Over the Air	438
Denial of Service	439
Summary	439
Endnotes	440

12 Hardware Perspectives for End-to-End Security (E2E) in Wireless Applications 443

Taxonomy of Communications Systems	444
Client-Server versus Peer-to-Peer	445
Circuit-Switched versus Packet-Switched or Frame-Switched Communications	446
Unicast versus Broadcast Communications	451
Land-Based versus Wireless-Based Communications	453
Transmission Medium (Non-LAN Point-to-Point, LAN or WAN, or LAN-WAN-LAN)	455
Transmission Nature: Voice versus Data (Audio, Video, Alphanumeric)	456
Quantity, Speed, and Predictability of Transmitted Information	462
Protocol Sensitive Communications Security	463
Evolution Towards Wireless (HW and SW Avenues)	468
Encryptor Structures in Wireless	468
Interception and Vulnerability of Wireless Systems	470
Communications ESM and Interception Receivers	473
CVR	473
IFM	474
YIG-Tuned Narrowband Superheterodyne	474
YIG-Tuned Wideband Superheterodyne	475
Spectral Analyzer ESM Receiver	475
Channelized Receiver	476
Compressive Receiver	476
Acousto-Optical Bragg Cell Receiver	476
SAW Technology	477

Direct-Sequence Spread-Spectrum Systems Interception	481
Frequency-Hopping Systems Interception	482
Modulation Recognition and Comint System Output Processing	487
Decision Theoretical Approach	490
Analog-Modulated Signals	491
Digitally modulated signals	491
Neural-Network-Based Approach	493
Implications	493
Advanced Mobile Phone Services (AMPS)	493
Time Division Multiple Access (TDMA) IS-136	494
GSM	494
Wideband and narrowband CDMA	495
Covert Transmission	496
Conclusions	497
Endnotes	498

13 Optimizing Wireless Security with FPGAs and ASICs 503

Optimizing? Yes, But What?	503
The 'Trust Nobody' Design Mentality	505
Evaluating Secure Design Architectures	506
'Weasel' Model Philosophy and Rationale	507
A Case Study	508
Software vs. Hardware Implementation of Wireless Security	512
Configurable versus Non-Configurable Hardware	515
Configurable Logic Blocks	519
Distributed Arithmetic	522
FPGA vs. ASIC Approach in the Design Trade-Offs:	
A Business Context	522
On-Chip Modules Provide Wireless Communications Security	524
Required Modules in a Block-Cipher-Based COMSEC Chip	525
Basic Architectures for Block-Cipher Crypto Engines in a COMSEC Chip	527
Transmission Comparison of Cryptographic Modes of Operation	527
Security Considerations for the Modes During Transmission	527
Recovery Properties for Garbled and Dropped Bits	530
Block Size and Communications Protocol	530
Comparison Matrix for Performance Optimization	530
Basic Architectures for Block-Cipher Crypto Engines in a COMSEC Chip	532
Comparison of the Block-Cipher Implementation Architectures	535
Required Modules in a Stream-Cipher Based COMSEC Chip	537
Protection Against Catalog Attacks	540
Protection Against Power Analysis Attacks	540
Protection Against Traffic Analysis Attacks	541
Common Techniques for Implementing Security Modules	542
Initialization Vectors and Random Number Generation	543

The Case of Stream Ciphers	543
Embedded Generation of Random Numbers	545
LFSR- and Linear Congruence-Based Schemes	545
User-Initiated Information Collection	545
Nonlinear Diode-Based RNG	546
Ambient Noise-Based RNG	547
Sampling White Noise	547
Chaotic Processing-Based RNG	548
Intel's Embedded RNG Source	548
IBM Embedded RNG Source	551
Other Designs	552
Binary Number Multiplication and Accumulation Engine	553
Modular Arithmetic Unit and Exponentiation Engine	553
Hashing	555
Diffie-Hellman (DH) Key Exchange	558
Elliptic-Curve-Cryptography-Based Diffie-Hellman and Digital Signatures	560
Hyperelliptic Curves	561
NTRU Lattice Cryptography Engine	562
NTRU Key Generation	563
NTRU-Based Encryption	563
NTRU-Based Decryption	563
Other Alternative Techniques	564
RPK Key Protocol	565
Secure Repacketization of Information	565
Kasumi Algorithm	568
Hardware-Efficient Rijndael Implementations and Comparison with Alternative Technologies	572
Power Consumption versus Performance	574
Software Implementations of Rijndael in an SOC	575
Comparing Rijndael with HORNET™ and DES/3DES in Embedded SW	578
Implementation of Rijndael on Configurable Hardware	579
Full-Custom VLSI Hardware Implementations	583
Authentication in Third-Generation Handsets	586
Conclusions	587
Endnotes	587

Bibliography 595

Trademarks	637
Unpublished Articles	638
Public Documents	638

Index 639