

# Index

- 3DES process, 108–109
- 3G devices
  - books about, 82
  - definition, 7
- 802.11 standard
  - access points, 40
  - ad hoc mode, 41–43
  - architecture modes, 41–43
  - bridging, 40
  - BSS (basic service set), 41–43
  - collision detection, 44–45
  - components, 40
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 44–45
  - distribution systems, 41–43
  - ESS (extended service set), 41–43
  - infrastructure mode, 41–43
  - MAC (Media Access Control) layer, 44–45
  - stations, 40
- 802.11b standard. *See also* WEP (Wired Equivalent Privacy) protocol.
  - advantages, 39
  - Barker sequences, 44
  - basic features, 12–13
  - chips, 44
  - clipping, 44
  - data rates, 43–44
  - description, 12–13
  - DSSS (direct-sequence spread spectrum), 43–44
  - FHSS (frequency-hopping spread spectrum), 43–44
  - physical layer, 43–44
  - security exposures, 12–13
  - signaling methods, 43–44
  - speed, 43–44
  - symbols, 44
  - vs.* Bluetooth, 15–16
  - waveforms, 44
- 911 access
  - E911 privacy policy, 154–156
  - tracking user locations, 154–157, 160
  - Wireless Communication and Public Safety Act of 1999, 156–157
- access control and authorization principle, 23
- access element, 81
- access points
  - definition, 40
  - security issues, 47–48
- accessories for devices. *See* expanding devices.
- accountability. *See* nonrepudiation.
- accuracy of data. *See* integrity.
- ACK (explicit packet acknowledgment), 44–45
- ACL (Asynchronous Connectionless) links, 52
- active attacks, 106
- ad hoc mode, 41–43
- add-ons for devices. *See* expanding devices.
- Address Book, Blackberry, 72
- administrative servers
  - protections, 222–227
  - vulnerabilities, 172, 196–198
- AES (Advanced Encryption Standard), 109
- analyze attacks. *See also* analyze attacks; analyze vulnerabilities; generate

- analyze attacks (*continued*)
  - protections; identify roles; identify targets.
  - denial of service, 188–189
  - description, 32
  - device theft, 188
  - DoCoMo e-mail virus, 189
  - known, 187–189
  - man-in-the-middle, 188
  - theoretical, 189
  - war driving, 188
- Analyze attacks and vulnerabilities phase, 32.
  - See also* analyze attacks; analyze vulnerabilities.
- analyze traffic, 102–103
- analyze vulnerabilities. *See also* analyze attacks; generate protections; identify roles; identify targets.
  - backend server, 203
  - corporate data, 191, 197–198, 199, 201–202
  - description, 32
  - gateways, 173–175, 199–202
  - service providers
    - administrative servers, 196–198
    - network server, 198–199
    - subscriber access, 195–196
    - transceivers, 195, 196
  - third-party data. *See* analyze vulnerabilities, corporate data.
  - user-specific data, 196–197, 198–199, 200–201
  - Web server, 203
  - wireless devices
    - data loss, sent data, 192–194
    - data loss, stored data, 190–191
    - network access, 193–194
    - offline functions, 190–191
    - online functions, 192–194
    - online service access, 193–194
    - PDA's (Personal Digital Assistants), 190–191
    - physical device, 190
    - transceivers, 194
    - user interface, 190
    - user location and movement, 193
    - user online activities, 193
- Anti-Terrorism Act, 157–158
- application developers, malicious programmers, 176
- protections
  - corporate data, 212–213, 225–226, 228
  - network access, 216
  - online service access, 216
  - personal data, 208–209
  - subscriber access, 220–221
  - user-specific data, 223, 227–228
- vulnerabilities
  - administrative servers, 197
  - gateways, 200–202
  - network access, 194
  - network servers, 198, 199
  - online functions, 193
  - online service access, 194
  - personal PDA data, 191
  - service provider, 196
- application layer, 143
- application security, 231–232
- application support personnel, malicious
  - protections
    - corporate data, 213–214, 226, 229
    - personal data, 209–210
    - subscriber access, 221–222
    - user-specific data, 223–224, 228
  - vulnerabilities
    - administrative servers, 197, 198
    - gateways, 200–202
    - network servers, 198, 199
    - online functions, 193
    - personal PDA data, 191
    - service provider, 196
- architecture. *See also* wireless devices.
  - 802.11 standard, 41–43
  - bearers, 4
  - Bluetooth, 52–53
  - conference model, 4
  - generic model, 4
  - Internet bridges, 5
  - multipurpose phone model, 4
  - synchronizer model, 4
  - towers, 4
  - usage models, 4–6
  - wireless gateways, 4
- asymmetric cryptography. *See* cryptography, asymmetric.
- Asynchronous Connectionless (ACL) links, 52
- attackers. *See* application developers; application support personnel; content

- providers; device support personnel;  
identify roles (of attackers); OMS  
personnel; users, malicious.
- attacks
  - analyzing. *See* analyze attacks.
  - chronological history, xi–xii
  - cryptography
    - active, 106
    - brute-force, 111–112
    - buffers, 127
    - information leakage, 127
    - man-in-the-middle, 127
    - misuse, 124–127
    - passive, 106
    - traffic analysis, 102–103
  - denial of service, 188–189
  - device theft, 188, 207
  - DoCoMo e-mail virus, 189
  - known, 187–189
  - man-in-the-middle, 188
  - predicting, 78
  - targets. *See* identify targets.
  - theoretical, 189
  - war driving, 188
- auditing principle, 25–26
- authenticated key establishment protocol,  
122
- authentication
  - biometric, 146–147
  - LMP (Link Manager Protocol), 52–53
  - vs.* encryption, 126–127
  - WEP (Wired Equivalent Privacy) protocol,  
46–47
  - WTLS (Wireless Transport Layer Security),  
57
- authentication principle, 22–23
- authorization. *See* access control and  
authorization.
- AutoText feature, 71
- backend server, vulnerabilities, 203
- Barker sequences, 44
- Baseband and Link Control (BLC) protocol,  
52–53
- basic service set (BSS), 41–43
- battery life
  - Blackberry, 70–71
  - consumer issues, 9
  - Palm OS, 66
  - Pocket PC, 68
  - power management, 69
- bearers, 4
- biometric authentication, 146–147
- birthday paradox, 111–112
- Blackberry
  - Address Book, 72
  - APIs, 71–72
  - AutoText feature, 71
  - battery life, 70–71
  - Database API, 71–72
  - encryption, 73
  - expanding, 65
  - input devices, 71
  - passwords, 73
  - Radio API, 71–72
  - security, 72–74
  - self destruct, 73
  - User Interface API, 71–72
- blanket permission, 60
- BLC (Baseband and Link Control) protocol,  
52–53
- block ciphers, 107–109
- Bluetooth
  - ACL (Asynchronous Connectionless)  
links, 52
  - architecture, 52–53
  - avoiding interference, 49
  - BLC (Baseband and Link Control) protocol,  
52–53
  - Cable Replacement Protocol, 53
  - cost, 15, 48–49
  - data services, 52–53
  - description, 15–16
  - discoverable mode, 53
  - frequency-hopping, 49
  - Generic Access Protocol, 54–55
  - history of, 15
  - inquiry messages, 50
  - L2CAP (Logical Link Control and  
Adaptation Protocol), 52–53
  - limitations, 52
  - LMP (Link Manager Protocol), 52–53
  - master devices, 49
  - operating range, 49, 54
  - page messages, 50
  - physical layer, 49–52
  - physical links, 52
  - piconets

- Bluetooth (*continued*)
  - definition, 49
  - forming, 52
  - joining, 50–52
  - point-to-multipoint communication, 50
  - point-to-point communication, 50
  - profiles, 53–55
  - protocols, 52–53
  - scatternets, 50–51
  - SCO (Synchronous Connection-Oriented)
    - links, 52
  - SDP (Service Discovery Protocol), 52–53
  - security issues, 15–16
  - security modes, 54–55
  - slave devices, 49
  - slots, 49
  - Telephony Control Protocol, 53
  - vs.* 802.11b, 15–16
- Bluetooth Special Interest Group, 48
- books about
  - 3G wireless applications, 82
  - cryptography, 99
  - GPRS, 82
  - Palm programming, 82
  - software security, 83
  - WML (Wireless Markup Language), 82
- bridging, 40
- browsers. *See* Web browsers.
- brute-force attacks, 111–112
- BSS (basic service set), 41–43
- Building Secure Software*, 83
- bytecodes
  - J2ME, 87–88
  - WML (Wireless Markup Language), 80
- Cable Replacement Protocol, 53
- CALEA (Communications Assistance for Law Enforcement Act), 154
- California privacy legislation, 152
- cards, 79–80
- carnivore. *See* DCS1000
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), 44–45
- case studies
  - home, 19–20, 243–245
  - hospital, 17–18, 235–239
  - office, 18–19, 100–103, 239–241
  - university, 19, 241–243
- CBC (Cipher Block Chaining) mode, 114
- CDC (Connected Device Configuration), 94–95
- cell phones, 6–7. *See also* wireless devices.
- Cellular Telecommunication Industry Association (CTIA), 160–161
- Certificates protocol, 121–122
- chips (802.11b), 44
- chronology of issues and attacks, xi–xii
- Cipher Block Chaining (CBC) mode, 114
- classes, J2ME
  - differences, 90–91
  - file format, 87
  - loader, 87–88
  - system class loaders, 87–88
  - user class loaders, 88
  - verifier, 88
- CLDC (Connected Limited Device Configuration), 92–94
- clipping, 44
- closed systems, 10
- collision detection, 44–45
- commercial off-the-shelf (COTS) products. *See* COTS (commercial off-the-shelf) products.
- Communications Assistance for Law Enforcement Act (CALEA), 154
- CompactFlash card, 65
- conduits, 66
- conference model, 4
- confidentiality principle, 24
- configurations, J2ME, 92–95
- confirming packet receipt, 44–45
- Connected Device Configuration (CDC), 94–95
- Connected Limited Device Configuration (CLDC), 92–94
- consumer issues, 8–10
- content providers, malicious
  - protections, 220
  - vulnerabilities, 196
- context permission, 60
- corporate data
  - protections, 211–214, 219, 224–229
  - vulnerabilities, 197–198, 199, 201–202
- corporate servers
  - protections, 219
  - vulnerabilities, 195
- cost principle, 29

- costs
  - Bluetooth, 15, 48–49
  - of cryptographic attacks, 106
  - devices, 6
  - WLANs (wireless local area networks), 16
- COTS (commercial off-the-shelf) products
  - biometric authentication, 146–147
  - IPSec, 144–145
  - SmartCards, 145–146
  - tunneling, 141–144
  - VPNs (Virtual Private Networks)
    - definition, 135
    - example topologies, 135–140
    - firewall-based, 139
    - hardened, 139
    - hardware-based, 138–139
    - multi-protocol, 143–144
    - software-based, 140–141
  - vs.* custom software, 133–135
- Counter (CTR) mode, 114–116
- cracking. *See* attacks.
- cross-platform communication, 10
- cross-platform independence. *See* J2ME.
- cryptography. *See also* encryption.
  - AES (Advanced Encryption Standard), 109
  - asymmetric
    - authenticated key establishment protocol, 122
    - Certificates protocol, 121–122
    - definition, 105
    - Diffie-Hellman problems, 117–119
    - Digital Signatures protocol, 121
    - discrete logarithms, 117–119
    - elliptic curve discrete algorithms, 119
    - Encryption protocol, 120–121
    - key agreement protocol, 122
    - Key Establishment protocol, 121–122
    - key transport protocol, 121
    - perfect forward secrecy, 122
    - PKI (public key infrastructure), 122
    - primitives, 116–119
    - protocols, 119–122
    - RSA technique, 116–117
  - attacks
    - active, 106
    - brute-force, 111–112
    - buffers, 127
    - information leakage, 127
    - L2TP (Layer Two Tunneling Protocol), 144
    - man-in-the-middle, 127
    - misuse, 124–127
    - passive, 106
    - PPTP (Point-to-Point Tunneling Protocol), 143–144
    - steganography, 24
    - traffic analysis, 102–103
  - choosing an algorithm, 127–130
  - ciphertext messages, 102
  - costs of attacks, 106
  - creating your own, 123–124
  - decryption, 102
  - digital signatures, 103
  - effectiveness, 128–129
  - encryption, 102
  - hash functions, 111–112
  - key agreement algorithm, 103
  - key agreement protocol, 122
  - Key Establishment protocol, 121–122
  - key transport protocol, 121
  - keys
    - and block ciphers, 108
    - definition, 103
    - generating, 124–125
    - managing, 125–126
    - multi-key encryption/decryption. *See* cryptography, asymmetric.
    - public, 116–117, 119
    - randomization, 125
    - RSA, 116–117
    - single-key encryption/decryption. *See* cryptography, symmetric.
    - suggested length, 129
  - keystream generator, 110–111
  - keystream reuse, 126
  - large numbers, 106–107
  - MAC (message authentication code), 103
  - misuses, 124–127
  - one-time pad, 109–110
  - performance, 128
  - plaintext messages, 102
  - primitives, 103
  - problems with, 122–124
  - protocols, 103
  - random numbers, 111
  - Rijndael cipher, 109
  - steganography, 24
  - stream ciphers, 109–111

- cryptography (*continued*)
  - symmetric
    - 3DES process, 108–109
    - block ciphers, 107–109
    - CBC (Cipher Block Chaining) mode, 114
    - CTR (Counter) mode, 114–116
    - definition, 104
    - DES process, 108
    - ECB (Electronic Code Book) mode, 113
    - encryption mode, 112–113
    - MACs (message authentication codes), 116
    - primitives, 107–112
    - protocols, 112–116
    - randomized CTR mode, 114–116
    - stateful CTR mode, 114–116
    - tagging algorithm, 116
    - three-key 3DES, 109
    - triple-DES process, 108–109
    - verification algorithm, 116
  - traffic analysis, 102–103
  - two-key 3DES, 109
  - types of attacks, 105–106
  - Vernam one-time pad, 109–110
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 44–45
- CTIA (Cellular Telecommunication Industry Association), 160–161
- CTR (Counter) mode, 114–116
- custom software
  - vs.* COTS (commercial off-the-shelf) products, 133–135
  - vulnerabilities, 134–135
- data
  - integrity principle, 25
  - protections
    - corporate data, 211–214, 224–229
    - losing sent data, 211–214
    - personal data, 208–210, 211–214
    - user-specific data, 222–224, 227–228
  - vulnerabilities
    - corporate data, 197–198, 199, 201–202
    - losing sent data, 192–194
    - losing stored data, 190–191
    - user-specific data, 196–197, 198–199, 200–201
- data link layer, 141
- data rates, 802.11b, 43–44
- data services, Bluetooth, 52–53
- Database API, 71–72
- DCS1000 (e-mail tracking system), 151, 157–158
- decks
  - description, 79–80
  - protecting access to, 81–82
  - self-contained, 80
  - sending cards to, 80
- decryption
  - definition, 102
  - multi-key. *See* cryptography, asymmetric.
  - single-key. *See* cryptography, symmetric.
- define strategies. *See also* development process.
  - home case study, 243–244
  - hospital case study, 235–239
  - office case study, 230–241
  - university case study, 241–243
- Define strategies phase, 32
- denial of service attacks, 188–189
- DES process, 108
- design security. *See also* development process.
  - home case study, 243–244
  - hospital case study, 235–239
  - office case study, 230–241
  - university case study, 241–243
- Design security phase, 32–33
- designers, malicious, 176
- developers, malicious. *See* application developers, malicious.
- development process. *See also* analyze attacks; analyze vulnerabilities; define strategies; design security; generate protections; I-ADD; identify roles; identify targets.
  - Bluetooth profiles, 53–54
  - factors affecting, 8
  - principles. *See* principles, development and operation.
  - trade-offs, 26–27
- device support personnel, malicious protections
  - corporate data, 211–212
  - network access, 215
  - online service access, 215
  - personal data, 208

- vulnerabilities
  - network access, 194
  - online functions, 192
  - online service access, 194
  - personal PDA data, 191
- device theft, 188
- devices. *See* wireless devices.
- Diffie-Hellman problems, 117–119
- digital signatures
  - definition, 103
  - RSA technique, 116–117
- Digital Signatures protocol, 121
- direct-sequence spread spectrum (DSSS), 43–44
- discoverable mode, 53
- discrete logarithms, 117–119
- distribution systems, 41–43
- DNS spoofing, 86
- DoCoMo e-mail virus attacks, 189
- Dragonball processor, 66
- DSSS (direct-sequence spread spectrum), 43–44
- e-mail, tracking, 151, 157–158
- E911 privacy policy, 154–156
- eavesdropping, 154, 157–158
- ECB (Electronic Code Book) mode, 113
- efficiency principle, 28
- 802.11 standard
  - access points, 40
  - ad hoc mode, 41–43
  - architecture modes, 41–43
  - bridging, 40
  - BSS (basic service set), 41–43
  - collision detection, 44–45
  - components, 40
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 44–45
  - distribution systems, 41–43
  - ESS (extended service set), 41–43
  - infrastructure mode, 41–43
  - MAC (Media Access Control) layer, 44–45
  - stations, 40
- 802.11b standard. *See also* WEP (Wired Equivalent Privacy) protocol.
  - advantages, 39
  - Barker sequences, 44
  - basic features, 12–13
  - chips, 44
  - clipping, 44
  - data rates, 43–44
  - description, 12–13
  - DSSS (direct-sequence spread spectrum), 43–44
  - FHSS (frequency-hopping spread spectrum), 43–44
  - physical layer, 43–44
  - security exposures, 12–13
  - signaling methods, 43–44
  - speed, 43–44
  - symbols, 44
  - vs.* Bluetooth, 15–16
  - waveforms, 44
- Electronic Code Book (ECB) mode, 113
- elliptic curve discrete algorithms, 119
- encryption. *See also* cryptography; WEP (Wired Equivalent Privacy) protocol.
  - Blackberry, 73
  - definition, 102
  - LMP (Link Manager Protocol), 52–53
  - multi-key. *See* cryptography, asymmetric.
  - Palm OS, 67–68
  - passwords, 67–68
  - single-key. *See* cryptography, symmetric.
  - vs.* authentication, 126–127
- encryption mode, 112–113
- Encryption protocol, 120–121
- ESS (extended service set), 41–43
- European Union (EU), 160
- examples and exercises. *See* case studies.
- expanding devices
  - Blackberry, 65
  - consumer issues, 9
  - memory expansion, 64–65
  - PDA (Personal Digital Assistants), 64–65
  - PocketPC, 65
  - storage expansion, 64–65
  - WLANs (wireless local area networks), 16
- explicit packet acknowledgment (ACK), 44–45
- exposures, analyzing. *See* I-ADD.
- extended service set (ESS), 41–43
- Fast Packet Keying solution, 48
- FCC, role in privacy, 154–156
- FHSS (frequency-hopping spread spectrum), 43–44
- financially motivated attackers, 175–176

- firewall-based VPNs, 139
- flash memory, 64–65
- Foundation Profile, 96
- Fourth Amendment implications, 159
- frequency-hopping, 49
- frequency-hopping spread spectrum (FHSS), 43–44
- functionality principle, 27
  
- garbage collector, 87, 91
- gateways
  - definition, 4
  - protections, 229
  - vulnerabilities, 173–175, 199–202
- generate protections. *See also* analyze vulnerabilities.
  - application developers, malicious
    - corporate data, 212–213, 225–226, 228
    - network access, 216
    - online service access, 216
    - personal data, 208–209
    - subscriber access, 220–221
    - user-specific data, 223, 227–228
  - application security, 231–232
  - application support personnel, malicious
    - corporate data, 213–214, 226, 229
    - personal data, 209–210
    - subscriber access, 221–222
    - user-specific data, 223–224, 228
  - content providers, malicious, 220
  - corporate data, 211–214, 224–229
  - description, 32
  - device support personnel, malicious
    - corporate data, 211–212
    - network access, 215
    - online service access, 215
    - personal data, 208
  - gateways, 229
  - loss of devices, 206
  - network access, 215–216
  - network server, 227–229
  - OMS personnel, malicious
    - corporate data, 212, 225, 228
    - network access, 215–216
    - online service access, 215–216
    - service providers, 217–218
    - subscriber access, 219–220
    - transceivers, 217–218
    - user-specific data, 222–223, 227
  - online service access, 215–216
  - personal data, 208–210
  - prioritizing protections, 229–231
  - sent data, corporate, 211–214
  - service providers
    - administrative servers, 222
    - corporate and private servers, 219
    - corporate data, 211, 224–227
    - subscriber access, 219–222
    - transceivers, 217–219, 222
    - user-specific data, 222–227
  - theft of devices, 207
  - tracking user online activities and location, 214–215
  - user interface access, 207
  - user-specific data
    - administrative servers, 222–227
    - network server, 227–228
  - users, malicious
    - corporate data, 214, 227, 229
    - network access, 216
    - online service access, 216
    - personal data, 210
    - service providers, 218
    - subscriber access, 222
    - transceivers, 217–219
    - user-specific data, 223–224, 228
- Generic Access Protocol, 54–55
- GoAmerica, 70
- GPRS and 3G Wireless Applications*, 82
- GPS, 158–160
- Gramm-Leach-Bliley Act, 150
- Graphics, Windowing and Events Subsystem (GWES), 69
- GUI applications, Palm OS, 66–67
- guidelines. *See* principles.
- GWES (Graphics, Windowing and Events Subsystem), 69
  
- hackers, 175. *See also* application developers; application support personnel; content providers; device support personnel; identify roles (of attackers); OMS personnel; users, malicious.
- hacking. *See* attacks.
- hardened VPNs, 139
- hardware. *See* wireless devices.
- hardware-based VPNs, 138–139
- hash functions, 111–112



- HGW (Home Gateway), 144
- history of issues and attacks, xi–xii
- holsters, 206
- home case study, 19–20, 243–245
- Home Gateway (HGW), 144
- horizontal clickstreams, 80
- hospital case study, 17–18, 235–239
- I-ADD, 30–34. *See also* analyze attacks; analyze vulnerabilities; define strategies; design security; generate protections; identify roles; identify targets.
- identify roles (of attackers)
  - academics, 176
  - application developers
    - access to network and online services, 194
    - administrative servers, 197
    - gateways, 200–202
    - network servers, 198, 199
    - online functions, 193
    - personal PDA data, 191
    - service provider, 196
  - application support personnel
    - administrative servers, 197, 198
    - gateways, 200–202
    - network servers, 198, 199
    - online functions, 193
    - personal PDA data, 191
    - service provider, 196
  - content providers, 196
  - description, 31
  - designers, 176
  - device support personnel
    - access to network and online services, 194
    - online functions, 192
    - personal PDA data, 191
  - financially motivated, 175–176
  - hackers, 175
  - malicious users
    - access to network and online services, 194
    - administrative servers, 197, 198
    - definition, 175–176
    - gateways, 200–202
    - network servers, 199, 199
    - online functions, 193
    - personal PDA data, 191
    - service provider, 195, 196
    - transceivers, wireless device, 194
  - mapping roles to targets, 177–187
  - nonfinancially motivated, 175
  - OMS personnel
    - access to network and online services, 194
    - administrative servers, 197
    - gateways, 200–202
    - network servers, 198, 199
    - online functions, 193, 194
    - service provider, 195
  - organized crime, 175
  - programmers, 176
  - security researchers, 176
- identify targets
  - description, 31
  - mapping targets to roles, 177–187
  - service providers
    - administrative servers, 172
    - corporate and private servers, 195
    - gateways, 173–175
    - network servers, 172–173
    - OMS personnel, 195
    - transceivers, 171–172
    - WSPs (Wireless Service Providers), 192
  - wireless devices
    - offline functions, 169
    - online functions, 169
    - physical devices, 165–168
    - transceivers, 169–170
    - user interface, 168–169
- Identify targets and roles phase, 31
- identifying users. *See* authentication; nonrepudiation.
- IEEE standards. *See* 802.11b standard.
- information leakage, 127
- infrared (IR) communication, 14
- infrastructure mode, 41–43
- input devices
  - AutoText feature, 71
  - Blackberry, 71
  - consumer issues, 8
  - keyboard, 71
  - Palm OS, 66–67
  - stylus, 66–67
  - touch screen, 66–67
- inquiry messages, 50
- integrity principle, 25

- interference, avoiding, 49
- Internet bridges, 5
- Introduction to Applied Cryptography*, 99
- IPSec, 144–145
- IR (infrared) communication, 14
  
- J2ME
  - bytecodes, 87–88
  - CDC (Connected Device Configuration), 94–95
  - class differences, 90–91
  - class file format, 87
  - class loader, 87–88
  - class verifier, 88
  - CLDC (Connected Limited Device Configuration), 92–94
  - components, 87
  - configurations, 92–95
  - for consumer electronics. *See* CDC (Connected Device Configuration).
  - for embedded devices. *See* CDC (Connected Device Configuration).
  - Foundation Profile, 96
  - freeing memory, 87, 91
  - future of, 96
  - garbage collector, 87, 91
  - history of, 90
  - Java Community Process*, 89
  - Java runtime libraries, 88
  - java.lang package, 88
  - javap tool, 87
  - JRE (Java Runtime Environment), 87
  - JVM (Java Virtual Machine), 87
  - JVMS (Java Virtual Machine Specifications), 87
  - K virtual machine, 90–91
  - KVM, 90–91
  - MIDP (Mobile Information Device Profile), 95–96
  - naming conventions, 89
  - native code interface, 88
  - off-device verification, 93
  - preverification, 93
  - profiles, 92, 95–96
  - for resource-constrained devices. *See* CLDC (Connected Limited Device Configuration).
  - standard extensions, 89
  - system class loaders, 87–88
  - user class loaders, 88
  - versions, 86–87
  - Web site for, 96
- Java 2 Enterprise Edition, 90
- Java 2 Standard Edition, 90
- Java Community Process*, 89
- Java language. *See* J2ME.
- Java Runtime Environment (JRE), 87
- Java runtime libraries, 88
- Java Virtual Machine (JVM), 87
- Java Virtual Machine Specifications (JVMS), 87
- JavaCard, 145
- java.lang package, 88
- javap tool, 87
- JRE (Java Runtime Environment), 87
- JVM (Java Virtual Machine), 87
- JVMS (Java Virtual Machine Specifications), 87
  
- K virtual machine, 90–91
- key agreement algorithm, 103
- key agreement protocol, 122
- Key Establishment protocol, 121–122
- key transport protocol, 121
- keyboards, BlackBerry, 71
- keys (encryption)
  - and block ciphers, 108
  - definition, 103
  - generating, 124–125
  - managing, 125–126
  - multi-key encryption/decryption. *See* cryptography, asymmetric.
  - public, 116–117, 119
  - randomization, 125
  - RSA, 116–117
  - single-key encryption/decryption. *See* cryptography, symmetric.
  - suggested length, 129
- keystream generator, 110–111
- keystream reuse, 126
- known attacks, 187–189
- KVM, 90–91
  
- L2CAP (Logical Link Control and Adaptation Protocol), 52–53
- L2TP Access Concentrator (LAC), 144
- L2TP (Layer Two Tunneling Protocol), 144
- L2TP Network Server (LNS), 144
- LAC (L2TP Access Concentrator), 144

- languages. *See* J2ME; JavaCard; WML (Wireless Markup Language); WMLScript.
- laptops, wireless, 7–8
- large numbers, 106–107
- laws. *See* privacy legislation.
- Layer Two Tunneling Protocol (L2TP), 144
- legal issues. *See* privacy legislation.
- legislation. *See* privacy legislation.
- Link Manager Protocol (LMP), 52–53
- list of issues and attacks, xi–xii
- LMP (Link Manager Protocol), 52–53
- LNS (L2TP Network Server), 144
- location-based marketing, 158–160
- Logical Link Control and Adaptation Protocol (L2CAP), 52–53
- loss, device, 206
  
- MAC (Media Access Control) layer, 44–45
- MACs (message authentication codes), 103, 116
- maintainability principle, 28
- malicious attackers. *See* application developers; application support personnel; content providers; device support personnel; identify roles (of attackers); OMS personnel; users, malicious.
- man-in-the-middle attacks, 127, 188
- management principles. *See* principles, management.
- mapping roles to targets, 177–187
- margin principle, 30
- marketability principle, 30
- marketing
  - location-based, 158–160
  - privacy legislation, 158–160
  - push, 159
  - tracking user locations, 158–160
- master devices, 49
- Media Access Control (MAC) layer, 44–45
- memory
  - expanding, 64–65
  - flash memory, 64–65
  - freeing, 87, 91
  - SD (Secure Digital) Memory Cards, 65
- Memory Stick, 65
- message authentication codes (MACs), 103, 116
- MIDP (Mobile Information Device Profile), 95–96
- mitigations. *See* generate protections.
- Mobile Information Device Profile (MIDP), 95–96
- monitoring. *See* surveillance; tracking.
- MP3, PDA storage card, 65
- MultiMediaCard, 65
- multipurpose phone model, 4
  
- Neomar, 70
- network access
  - protections, 215–216
  - vulnerabilities, 193–194, 194
- network access server, 144
- network layer, 142
- network servers
  - protections, 227–229
  - vulnerabilities, 172–173, 198–199, 199
- networking technologies. *See* technologies.
- networks
  - PANs (personal area networks), 15–16
  - private networks, 137
  - VPNs (Virtual Private Networks)
    - definition, 135
    - example topologies, 135–140
    - firewall-based, 139
    - hardened, 139
    - hardware-based, 138–139
    - multi-protocol, 143–144
    - software-based, 140–141
  - WANs (wide area networks), 14
  - WLANs (wireless local area networks)
    - advantages, 16
    - cost, 16
    - definition, 14
    - scalability, 16
- news stories about security, xi–xii
- 911 access
  - E911 privacy policy, 154–156
  - tracking user locations, 154–157, 160
  - Wireless Communication and Public Safety Act of 1999, 156–157
- nonfinancially motivated attackers, 175
- nonrepudiation principle, 23–24
- Novarra, 70
  
- off-device verification, 93
- office case study, 18–19, 100–103, 239–241
- offline functions, vulnerabilities, 169, 190–191

- OMS personnel, malicious
  - protections
    - corporate data, 212, 225, 228
    - network access, 215–216
    - online service access, 215–216
    - service providers, 217–218
    - subscriber access, 219–220
    - transceivers, 217–218
    - user-specific data, 222–223, 227
  - vulnerabilities
    - administrative servers, 197
    - gateways, 200–202
    - network access, 194
    - network servers, 198, 199
    - online functions, 193, 194
    - online service access, 194
    - service provider, 195
- one-time pad, 109–110
- online functions, vulnerabilities, 169, 192–194
- online service access
  - protections, 215–216
  - vulnerabilities, 193–194, 194
- Open System Interconnection (OSI). *See* OSI (Open System Interconnection).
- operation principles. *See* principles, development and operation.
- opt-in *vs.* opt-out, 149–151
- opt-out ability, 150
- organized crime attackers, 175
- OSI model, 141–143
- OSI (Open System Interconnection). *See also* 802.11b standard.
  - application layer, 143
  - data link layer, 141. *See also* 802.11b standard.
  - layers, 40, 141–143
  - network layer, 142
  - physical layer. *See also* 802.11b standard.
    - Barker sequences, 44
    - Bluetooth, 49–52
    - chips, 44
    - clipping, 44
    - data rates, 43–44
    - definition, 141
    - DSSS (direct-sequence spread spectrum), 43–44
    - FHSS (frequency-hopping spread spectrum), 43–44
    - signaling methods, 43–44
    - speed, 43–44
    - symbols, 44
    - waveforms, 44
  - presentation layer, 143
  - session layer, 143
  - transport layer, 142
- packets
  - ACK (explicit packet acknowledgment), 44–45
  - collision detection, 44–45
  - confirming receipt of, 44–45
- page messages, 50
- pages, WAE. *See* cards; decks.
- Palm OS devices, 66–68
- Palm Programming: The Developer's Guide*, 82
- Palm Query Application (PQA), 66
- PANs (personal area networks), 15–16
- passive attacks, 106
- passwords. *See also* security.
  - Blackberry, 73
  - Palm OS, 67–68
  - RAS (Remote Access Service), 143–144
- path element, 81–82
- PC cards, 65
- PCMCIA cards, 65
- PDA's (Personal Digital Assistants). *See also* wireless devices.
  - adapters, 65
  - adding storage, 65
  - description, 6–7
  - expanding, 64–65
  - features, 64
  - memory expansion, 64–65
  - PC cards, 65
  - PCMCIA cards, 65
  - vulnerabilities, 190–191
- peer-to-peer communication, 9–10
- perfect forward secrecy, 122
- performance, cryptography, 128
- peripherals, 9. *See also* expanding devices.
- permissions, 60
- personal area networks (PANs), 15–16
- personal data, protections, 208–210, 211–214
- Personal Digital Assistants (PDAs). *See* PDAs (Personal Digital Assistants).
- Personal Information Managers (PIMs). *See* PDAs (Personal Digital Assistants).

- physical layer
  - 802.11b standard, 43–44
  - Barker sequences, 44
  - Bluetooth, 49–52
  - chips, 44
  - clipping, 44
  - data rates, 43–44
  - definition, 141
  - DSSS (direct-sequence spread spectrum), 43–44
  - FHSS (frequency-hopping spread spectrum), 43–44
  - signaling methods, 43–44
  - speed, 43–44
  - symbols, 44
  - waveforms, 44
- physical links, Bluetooth, 52
- piconets
  - definition, 49
  - forming, 52
  - joining, 50–52
- PIMs (Personal Information Managers). *See* PDAs (Personal Digital Assistants).
- PKI (public key infrastructure), 122
- plaintext messages, 102
- planning a system. *See* I-ADD.
- Pocket PC, 68–70
- point-to-multipoint communication, 50
- point-to-point communication, 50
- power management, 69. *See also* battery life.
- PPTP (Point-to-Point Tunneling Protocol), 143–144
- PQA (Palm Query Application), 66
- presentation layer, 143
- preverification, 93
- principles of
  - development and operation
    - efficiency, 28
    - functionality, 27
    - maintainability, 28
    - scalability, 28
    - software development trade-offs, 26–27
    - testability, 28–29
    - usability, 27–28
    - utility, 27
  - management
    - cost, 29
    - margin, 30
    - marketability, 30
    - schedule, 29
  - security
    - access control and authorization, 23
    - auditing, 25–26
    - authentication, 22–23
    - integrity, 25
    - nonrepudiation, 23–24
    - privacy and confidentiality, 24
  - prioritizing protections, 229–231
  - privacy. *See also* surveillance; tracking.
    - carnivore. *See* DCS1000
    - DCS1000 (e-mail tracking system), 151, 157–158
    - opt-in *vs.* opt-out, 149–151
    - players, 153
    - rental cars, surveillance of, 160
    - role of the FCC, 154–156
    - spam, 151
    - unwanted messages, 151
  - privacy and confidentiality principle, 24
  - privacy legislation
    - 911 access, 156–157
    - Anti-Terrorism Act, 157–158
    - CALEA (Communications Assistance for Law Enforcement Act), 154
    - California, 152
    - E911 privacy policy, 154–156
    - eavesdropping, 154
    - EU (European Union), 160
    - Fourth Amendment implications, 159
    - GPS, 158–160
    - Gramm-Leach-Bliley Act, 150
    - Ireland, 160
    - location-based marketing, 158–160
    - opt-out ability, 150
    - push marketing, 159
    - right to privacy, 152
    - tracking e-mail, 157–158
    - tracking user locations
      - for marketing, 158–160
      - for public safety, 154–157, 160
    - unlawful search and seizure, 159
    - U.S.A. Patriot Act of 2001, 157–158
    - Wireless Communication and Public Safety Act of 1999, 156–157
    - wiretapping, 154, 157–158

- privacy policies
  - CTIA (Cellular Telecommunication Industry Association), 160–161
  - guidelines for privacy protection, 160–161
- private networks, 137
- private servers
  - protections, 219
  - vulnerabilities, 195
- profiles
  - Bluetooth, 53–55
  - J2ME, 92, 95–96
- programmers, malicious, 176. *See also* application developers, malicious.
- programming languages. *See* J2ME; JavaCard; WML (Wireless Markup Language); WMLScript.
- protections. *See also* vulnerabilities.
  - administrative servers, 222–227
  - content providers, malicious, 220
  - corporate data, 211–214, 219, 224–229
  - corporate servers, 219
  - gateways, 229
  - generating. *See* generate protections.
  - network access, 215–216
  - network servers, 227–229
  - online service access, 215–216
  - personal data, 208–210, 211–214
  - prioritizing, 229–231
  - private servers, 219
  - service providers, 217–218
  - subscriber access, 219–222
  - surveillance, 214–215
  - theft, 207
  - tracking user location and movement, 214–215
  - tracking user online activities, 214–215
  - transceivers, 217–219, 222
  - user interface access, 207
  - user-specific data, 222–228
- protocols
  - asymmetric cryptography, 119–122
  - authenticated key establishment protocol, 122
  - BLC (Baseband and Link Control) protocol, 52–53
  - Cable Replacement Protocol, 53
  - Certificates protocol, 121–122
  - cryptography, 103
  - Digital Signatures protocol, 121
  - Encryption protocol, 120–121
  - Generic Access Protocol, 54–55
  - key agreement protocol, 122
  - Key Establishment protocol, 121–122
  - key transport protocol, 121
  - L2CAP (Logical Link Control and Adaptation Protocol), 52–53
  - L2TP (Layer Two Tunneling Protocol), 144
  - LMP (Link Manager Protocol), 52–53
  - PPTP (Point-to-Point Tunneling Protocol), 143–144
  - SDP (Service Discovery Protocol), 52–53
  - symmetric cryptography, 112–116
  - Telephony Control Protocol, 53
  - WAP (Wireless Application Protocol). *See also* WAE (Wireless Application Environment) layer.
    - browsers, 77–78
    - communication cycle, 57–58
    - description, 13
    - history of, 55–56
    - protocol stack, 56–57, 76–77
    - security issues, 61–62
    - telephony services, 60–61
    - WML (Wireless Markup Language), 57
    - WMLScript, 57, 59
    - WSP (Wireless Session Protocol) layer, 57
    - WTLS (Wireless Transport Layer Security), 57
    - WTP (Wireless Transaction Protocol) layer, 57
  - WEP (Wired Equivalent Privacy) protocol
    - algorithm, 45–46
    - authentication process, 46–47
    - security issues, 47–48
  - WSP (Wireless Session Protocol) layer, 57
  - WTP (Wireless Transaction Protocol) layer, 57
- proximity sensors, 206
- public key infrastructure (PKI), 122
- public safety
  - 911 access, 154–157
  - E911 privacy policy, 154–156
  - tracking user locations, 154–157, 160
  - Wireless Communication and Public Safety Act of 1999, 156–157

- pull architecture, 70
- push architecture, 70
- push marketing, 159
  
- Radio API, 71–72
- radio frequency (RF) communication, 14
- random keys, 125
- random numbers, 111
- randomized CTR mode, 114–116
- RAS (Remote Access Service), 143
- Remote Access Service (RAS), 143
- rental cars, surveillance of, 160
- reviewing activities. *See* auditing.
- RF (radio frequency) communication, 14
- Rijndael cipher, 109
- RIM 950/957. *See* Blackberry.
- RIM (Research in Motion), 70–74
- risks. *See* security issues; vulnerabilities.
  - analyzing. *See* analyze attacks; analyze vulnerabilities; I-ADD; identify roles; identify targets.
- roles, identifying. *See* identify roles; identify targets.
- RSA technique, 116–117
- rules for secure systems. *See* principles.
  
- safety issues
  - 911 access, 154–157
  - E911 privacy policy, 154–156
  - tracking user locations, 154–157, 160
  - Wireless Communication and Public Safety Act of 1999, 156–157
- scalability. *See* expanding devices.
- scalability principle, 28
- scatternets, 50–51
- schedule principle, 29
- SCO (Synchronous Connection-Oriented) links, 52
- screen size, limitations of, 8
- scripting. *See* J2ME; JavaCard; WML (Wireless Markup Language); WMLScript.
- SD (Secure Digital) Memory Cards, 65
- SDP (Service Discovery Protocol), 52–53
- Secure Digital (SD) Memory Cards, 65
- Secure Socket Layer (SSL). *See* WTLS (Wireless Transport Security) layer.
- security
  - analyzing. *See* I-ADD.
  - equivalent to wired. *See* WEP (Wired Equivalent Privacy) protocol.
  - passwords. *See* passwords.
  - planning for. *See* I-ADD.
  - principles. *See* principles of, security.
  - security issues. *See also* vulnerabilities.
    - Bluetooth, 15–16
    - L2TP (Layer Two Tunneling Protocol), 144
    - Palm OS, 67–68
    - PPTP (Point-to-Point Tunneling Protocol), 143–144
  - recent events, xi–xii
  - stream ciphers, 110–111
  - WAP browsers, 77–78
  - WAP (Wireless Application Protocol), 61–62
  - Web browsers, 85–86
  - WEP (Wired Equivalent Privacy) protocol, 47–48
  - wireless access points, 47–48
- security modes, Bluetooth, 54–55
- security researchers, malicious, 176
- server security
  - protections
    - administrative servers, 222–227
    - corporate and private servers, 219
    - network server, 227–229
  - vulnerabilities
    - administrative servers, 172, 196–198, 197, 198
    - backend servers, 203
    - corporate and private servers, 195
    - network servers, 172–173, 198–199
    - Web servers, 203
- Service Discovery Protocol (SDP), 52–53
- service providers
  - protections
    - administrative servers, 222
    - corporate data, 211, 219, 224–227
    - subscriber access, 219–222
    - transceivers, 217–219, 222
    - user-specific data, 222–227
  - vulnerabilities
    - administrative servers, 172, 196–198
    - gateways, 173–175
    - network servers, 172–173, 198–199
    - subscriber access, 195–196
    - transceivers, 171–172, 195, 196

- session layer, 143
- signaling methods, 43–44
- single-action permission, 60
- slave devices, 49
- sleds, 65
- slots, 49
- SmartCards, 145–146
- SmartMedia, 65
- software
  - commercial. *See* COTS (commercial off-the-shelf) products.
  - custom *vs.* COTS, 133–135
  - developing. *See* development process.
- software-based VPNs, 140–141
- Solid State Floppy Disk Card (SSFDCC), 65
- spam, 151
- speed, 802.11b, 43–44
- Springboard, 65
- spying. *See* surveillance.
- SSFDCC (Solid State Floppy Disk Card), 65
- SSL (Secure Socket Layer). *See* WTLS (Wireless Transport Layer Security).
- standards. *See* 802.11b standard; Bluetooth; WAP (Wireless Application Protocol).
- stateful CTR mode, 114–116
- stations
  - connection through access points, 41–43
  - definition, 40
  - direct interconnection, 41–43
- steganography, 24. *See also* cryptography; encryption.
- strategies, developing. *See* define strategies; Define strategies phase.
- stream ciphers, 109–111
- stylus, 66–67
- subscriber access
  - protections, 219–222
  - vulnerabilities, 195–196
- support personnel, malicious. *See* application support personnel; device support personnel.
- surveillance
  - carnivore. *See* DCS1000
  - DCS1000 (e-mail tracking system), 151, 157–158
  - issues, 152
  - protections, 214–215
  - of rental cars, 160
  - tracking e-mail, 151, 157–158
  - tracking user location and movement
    - for marketing, 158–160
    - protections, 214–215
    - for public safety, 154–157, 160
    - vulnerabilities, 193
  - tracking user online activities
    - protections, 214–215
    - vulnerabilities, 193
- symbols, 44
- symmetric cryptography. *See* cryptography, symmetric.
- synchronizer model, 4
- synchronizing Palm OS to desktop, 66
- Synchronous Connection-Oriented (SCO) links, 52
- system class loaders, 87–88
- tagging algorithm, 116
- targets, identifying. *See* identify roles; identify targets.
- technical issues, 10–11
- technologies. *See also* 802.11b standard; Bluetooth; WAP (Wireless Application Protocol).
  - IR (infrared) communication, 14
  - PANs (personal area networks), 15–16
  - RF (radio frequency) communication, 14
  - WANs (wide area networks), 14
  - wired WANs, 14
  - wireless WANs, 14
  - WLANs (wireless local area networks)
    - advantages, 16
    - cost, 16
    - definition, 14
    - scalability, 16
  - WTLS (Wireless Transport Layer Security), 13, 57
- Telephony Control Protocol, 53
- telephony services
  - permissions, 60
  - WMLScript, 84–85
  - WTA (Wireless Telephony Application), 59–61
  - WTAI (Wireless Telephony Application Interface), 60
- testability principle, 28–29
- theft of devices, 207



- theoretical attacks, 189
- third generation devices. *See* 3G devices.
- third-party products. *See* COTS (commercial off-the-shelf) products.
- 3DES process, 108–109
- 3G devices
  - books about, 82
  - definition, 7
- three-key 3DES, 109
- TLS (Transport Security Layer). *See* WTLS (Wireless Transport Layer Security).
- touch screen, Blackberry, 66–67
- towers, 4
- tracking e-mail, 151, 157–158
- tracking users. *See also* surveillance.
  - location and movement
    - for marketing, 158–160
    - protections, 214–215
    - for public safety, 154–157, 160
    - vulnerabilities, 193
  - online activities
    - protections, 214–215
    - vulnerabilities, 193
- traffic analysis, 102–103
- transceivers
  - protections, 217–219, 222
  - vulnerabilities, 169–172, 194–195
- transport layer, 142
- Transport Security Layer (TLS). *See* WTLS (Wireless Transport Layer Security).
- transportability, 9
- triple-DES process, 108–109
- tunneling, 141–144
- two-key 3DES, 109
  
- university case study, 19, 241–243
- unlawful search and seizure, 159
- unwanted messages, 151
- U.S.A. Patriot Act of 2001, 157–158
- usability principle, 27–28
- usage models, 4–6
- user agents, 59
- user class loaders, 88
- user interface access
  - protections, 207
  - vulnerabilities, 168–169, 190
- User Interface API, 71–72
  
- user location and movement, tracking. *See* tracking users.
- user roles, identifying. *See* identify roles; identify targets.
- user-specific data
  - protections, 222–228
  - vulnerabilities, 196–197, 198–199, 200–201
- users
  - accountability. *See* nonrepudiation.
  - identifying. *See* authentication; nonrepudiation.
  - multiple. *See* MAC (Media Access Control) layer.
  - reviewing activities. *See* auditing.
  - sharing media. *See* MAC (Media Access Control) layer.
  - tracking. *See* surveillance; tracking users.
  - verifying data accuracy. *See* integrity.
- users, malicious
  - academics, 176
  - definition, 175–176
  - designers, 176
  - financially motivated, 175–176
  - hackers, 175
  - nonfinancially motivated, 175
  - organized crime, 175
  - programmers, 176
  - protections
    - corporate data, 214, 227, 229
    - network access, 216
    - online service access, 216
    - personal data, 210
    - service providers, 218
    - subscriber access, 222
    - transceivers, 217–219
    - user-specific data, 223–224, 228
  - security researchers, 176
  - vulnerabilities
    - administrative servers, 197, 198
    - gateways, 200–202
    - network access, 194
    - network servers, 199, 199
    - online functions, 193
    - online service access, 194
    - personal PDA data, 191
    - service provider, 195, 196
    - transceivers, wireless device, 194
- utility principle, 27

- vendor products. *See* COTS (commercial off-the-shelf) products.
- verification algorithm, 116
- verifying data accuracy. *See* integrity.
- Vernam one-time pad, 109–110
- vertical clickstreams, 80
- Virtual Private Networks (VPNs). *See* VPNs (Virtual Private Networks).
- virus DoCoMo e-mail, 189
- Visor Edge, 66
- volumes (Pocket PC), 69–70
- VPNs (Virtual Private Networks)
  - definition, 135
  - example topologies, 135–140
  - firewall-based, 139
  - hardened, 139
  - hardware-based, 138–139
  - multi-protocol, 143–144
  - software-based, 140–141
- vulnerabilities. *See also* protections; security issues.
  - administrative servers, 172, 196–198, 197, 198
  - analyzing. *See* analyze attacks; analyze vulnerabilities; identify roles; identify targets.
  - backend server, 203
  - content providers, malicious, 196
  - corporate data, 197–198, 199, 201–202
  - custom software, 134–135
  - data loss, sent data, 192–194
  - data loss, stored data, 190–191
  - gateways, 173–175, 199–202
  - losing sent data, 192–194
  - losing stored data, 190–191
  - network access, 193–194, 194
  - network servers, 172–173, 198–199, 199
  - offline functions, 169, 190–191
  - online functions, 169, 192–194, 194
  - online service access, 193–194, 194
  - PDA's (Personal Digital Assistants), 190–191
  - service providers, 195, 195–196, 196
  - subscriber access, 195–196
  - transceivers
    - malicious users, 194
    - OMS personnel, 194
    - service providers, 171–172, 195
    - wireless devices, 169–170
  - user interface access, 168–169, 190
  - user-specific data, 196–197, 198–199, 200–201
  - Web server, 203
  - wireless devices
    - data loss, sent data, 192–194
    - data loss, stored data, 190–191
    - network access, 193–194
    - offline functions, 169, 190–191
    - online functions, 169, 192–194
    - online service access, 193–194
    - PDA's (Personal Digital Assistants), 190–191
    - physical devices, 165–168, 190
    - transceivers, 169–170, 194
    - user interface, 168–169, 190
    - user location and movement, 193
    - user online activities, 193
- WAE (Wireless Application Environment) layer
  - cards, 59
  - decks, 59
  - definition, 57
  - pages. *See* cards; decks.
  - user agents, 59
- WTA (Wireless Telephony Application), 59–61
- WTAI (Wireless Telephony Application Interface), 60
- WANs (wide area networks), 14
- WAP Forum, 55–56
- WAP (Wireless Application Protocol). *See also* WAE (Wireless Application Environment) layer.
  - browsers, 77–78
  - communication cycle, 57–58
  - description, 13
  - history of, 55–56
  - protocol stack, 56–57, 76–77
  - security issues, 61–62
  - telephony services, 60–61
- WML (Wireless Markup Language), 57
- WMLScript, 57, 59
- WSP (Wireless Session Protocol) layer, 57
- WTLS (Wireless Transport Layer Security), 13, 57

- WTP (Wireless Transaction Protocol) layer, 57
- war driving attacks, 188
- waveforms, 44
- WCA (Web clipping applications), 66
- wearable interfaces, 206
- Web browsers
  - GoAmerica, 70
  - Neomar, 70
  - Novarra, 70
  - Palm OS devices, 66–68
  - security issues, 85–86
  - WAP browsers, 77–78
- Web Clipping Application Viewer, 66
- Web clipping applications (WCA), 66
- Web pages
  - displaying. *See* WML (Wireless Markup Language).
  - displaying as text. *See* Palm OS devices.
- Web server, vulnerabilities, 203
- WEP (Wired Equivalent Privacy) protocol
  - algorithm, 45–46
  - authentication process, 46–47
  - security issues, 47–48
- wide area networks (WANs), 14
- Wired Equivalent Privacy (WEP) protocol. *See* WEP (Wired Equivalent Privacy) protocol.
- wired WANs, 14
- Wireless Application Environment (WAE) layer. *See* WAE (Wireless Application Environment) layer.
- Wireless Application Protocol, The*, 82
- Wireless Application Protocol (WAP). *See* WAP (Wireless Application Protocol).
- Wireless Communication and Public Safety Act of 1999, 156–157
- wireless devices. *See also entries for specific devices.*
  - 3G, 7, 82
  - access control. *See* access control and authorization.
  - authentication. *See* authentication; WEP (Wired Equivalent Privacy) protocol.
  - closed systems, 10
  - communication by pointing, 53
  - consumer issues, 8–10
  - cross-platform communication, 10
  - development factors, 8
  - discoverable mode, 53
  - expansion, 9
  - flash memory, 64–65
  - holsters, 206
  - identifying. *See* authentication.
  - input devices, 8
  - laptops, 7–8
  - MIDs (Mobile Information Devices), 95–96
  - operating range (Bluetooth), 49, 54
  - Palm OS, 66–68
  - peer-to-peer communication, 9–10
  - peripherals, 9
  - Pocket PC, 68–70
  - protecting information. *See* I-ADD.
  - proximity sensors, 206
  - reviewing activities. *See* auditing.
  - screen size, 8
  - sleds, 65
  - technical issues, 10–11
  - third generation, 7
  - transportability, 9
  - verifying data accuracy. *See* integrity.
  - vulnerabilities
    - data loss, sent data, 192–194
    - data loss, stored data, 190–191
    - network access, 193–194
    - offline functions, 169, 190–191
    - online functions, 169, 192–194
    - online service access, 193–194
    - PDAs (Personal Digital Assistants), 190–191
    - physical devices, 165–168, 190
    - transceivers, 169–170, 194
    - user interface, 168–169, 190
    - user location and movement, 193
    - user online activities, 193
    - wearable interfaces, 206
  - wireless gateways, 4
  - wireless local area networks (WLANs). *See* WLANs (wireless local area networks).
- Wireless Markup Language (WML). *See* WML (Wireless Markup Language).
- Wireless Session Protocol (WSP) layer, 57
- wireless technologies. *See* technologies.
- Wireless Telephony Application Interface (WTAD), 60
- Wireless Telephony Application (WTA), 59–61, 84–85
- Wireless Transaction Protocol (WTP) layer, 57
- Wireless Transport Layer Security (WTLS), 13, 57

- wireless WANs. *See* WANs (wide area networks).
- wiretapping, 154, 157–158
- WLANs (wireless local area networks)
  - advantages, 16
  - cost, 16
  - definition, 14
  - scalability, 16
- WML (Wireless Markup Language)
  - books about, 82
  - bytecode, 80
  - cards, 79–80
  - coding applications, 82–83
  - decks
    - description, 79–80
    - protecting access to, 81–82
    - self-contained, 80
    - sending cards to, 80
  - description, 79
  - displaying Web pages, 79–81
  - horizontal clickstreams, 80
  - specifications for, 82
  - vertical clickstreams, 80
- WMLScript
  - description, 83
  - DNS spoofing, 86
  - libraries, 84
  - security issues, 85–86
  - syntax, 84
  - telephony functions, 84–85
- WSP (Wireless Session Protocol) layer, 57
- WTA (Wireless Telephony Application), 59–61, 84–85
- WTAI (Wireless Telephony Application Interface), 60
- WTLS (Wireless Transport Layer Security), 13, 57
- WTP (Wireless Transaction Protocol) layer, 57