

INDEX

Numbers

401 error message, 27, 28
403 error response, 31–32
407 error message, 27, 28
802.lx devices, audit program, 194
911 services, VoIP and, 153

A

ACK (acknowledge) message
(SIP), 21
active dictionary attack, in IAX,
100–102
active eavesdropping of RTP, 82–87
 audio insertion, 82–86
 audio replacement, 87
AES (Advanced Encryption
 Standard)
 encryption limitations, 106
 secure RTP with cipher, 182
Aircrack, 175
anonymous eavesdropping,
 146–147
Apache build, security issues, 121
ARP cache poisoning, 38
ARP monitoring, audit
 program, 194
ARP Poison Routing menu (Cain &
 Abel), 79
ASN.1-encoded buffer, 58, 59
Asterisk servers, 26, 93, 132
 configuring, 4
 connecting SIP client to, 142
 for free calls, 138
 for IVR services for users, 136
 man-in-the-middle attack of,
 102–103
 to send pre-recorded messages,
 148–150
 SRTP implementation steps, 183
attack surface
 on home wireless devices, 156
 for RSA authentication, 94
audio files
 creating, 164
 recording with hard phone, 117
 from RTPInject, 85
 saving RTP stream to, 82
audio insertion
 in RTP eavesdropping, 82–86
 into Yahoo! Messenger calls, 170
audio replacement, in RTP
 eavesdropping, 87
audio RTP streams, capturing,
 76–77
auditing VoIP, for security best
 practices, 189–197
authentication, 13–14
 audit program, 193
 Denial of Service and, 67–68
 in Google Talk, 170
 for H.323 gatekeeper, 52
 in IAX, 94–96
 in SIP, 22, 27–29
 audit program, 190
 data collection for attacks, 34
 and Vonage, 166
authentication packet, generating, 61

- authorization
 - audit program, 193
 - for H.323 protocol, 54–55
 - in VoIP, 14
- AutoDiscovery, audit program, 196
- availability, in VoIP, 14–15
- Avaya
 - 4600 service hard phone,
 - settings from, 118
 - Call Center, 120–123
 - registering Asterisk
 - server to, 145
 - identifying TFTP server on
 - network, 116
 - Modular Messaging, 123–126
 - SRTP implementation steps, 183
 - TLS implementation steps, 181
 - VoIP hard phone, security
 - issues, 115–120
 - support for Yahoo! Messenger
 - RTP codecs, 169
 - call eavesdropping. *See*
 - eavesdropping
 - call redirection, 146–147
 - call reject attack, in IAX, 107–108
 - caller ID spoofing, 139–146
 - with iaxComm and VoIPJet,
 - 140–142
 - impact, 146
 - on internal network with VoIP
 - and SIP, 144–146
 - from services on websites,
 - 143–144
 - with SIP client, 142–143
 - Call-ID field (SIP), 21
 - CANCEL method (SIP), 21
 - for Denial of Service attack, 43
 - challenge (nonce), 27, 28, 29
 - challenge packet, from SIP
 - server, 166
 - Challenge Response Authentication Mechanism (CRAM-MD5), 124
 - challenge/response method, IAX
 - support for, 95
 - Cisco
 - CallManager, 120–123
 - registering Asterisk
 - server to, 145
 - SRTP implementation steps, 183
 - switches, hopping attacks
 - from, 66
 - TLS implementation steps, 181
 - VoIP hard phone
 - security issues, 115–120
 - sniffing network from, 115
 - cleartext transmission
 - IAX support for, 94
 - by RTP, 74, 76
 - of TFTP/HTTP requests, 117
 - with Vonage, 157
 - commercial VoIP solutions,
 - 154–167
 - Vonage, 154–161
 - conference calls
 - risks of audio replacement, 87
 - security for, 67

B

- BackTrack Live CD, 4
- baseline, for measuring VoIP, 190
- boot image, for hard phones, 117
- boot process, for hard phones,
 - audit program, 196
- brute-force attacks
 - of E.164 alias, 65–66
 - to gain valid usernames, 31–32
 - offline, 59
- buffer overrun attacks, IAX vs.
 - SIP, 94
- BYE message (RTP), 90
- BYE method (SIP), 21, 25
 - Denial of Service attack and,
 - 42–43

C

- Cain & Abel, 33, 36, 157, 175
 - for attack on Modular
 - Messaging, 125
 - to capture RTP packets, 158, 163
 - for RTP man-in-the-middle
 - attacks, 78–80, 159–160
 - for SSL man-in-the-middle
 - attacks, 171

- Contact field (SIP), 21
- Content-Length field (SIP), 21
- Content-Type field (SIP), 21
- contributing source for RTP (CSRC), 74
- Conversation Log, for spoofed BYE message, 43
- country code (CC), in E.164 alias, 14
- CRAM-MD5 (Challenge Response Authentication Mechanism), 124
- CSeq field (SIP), 21

D

- D-Link, 173
- data network, separating from voice network, 15
 - audit program, 194
- Denial of Service attack. *See* DoS attack
- DHCP servers, audit program, 197
- dictionary attack
 - active, in IAX, 100–102
 - offline, 33, 35, 58, 166, 180
 - in IAX, 97–100
- Diffie-Hellman (DH) key agreement, ZRTP and, 183
- digest authentication, to SIP server, 28, 180
- digital phones, 11
- disconnecting calls in progress, HangUP attack to cause, 108–109
- display language, hard phone configuration, 118
- DNS server
 - audit program, 197
 - hard phone configuration, 118
 - lookup by Proxy server, 23
- DNS spoofing techniques, 38
- DoS (Denial of Service) attack, 88–91
 - for H.323 protocol
 - via H.225
 - nonStandardMessage, 71–72
 - via host unreachable packets, 70–71
 - via NTP, 67–68
 - via UDP, 68–69
 - in IAX, 106–110
 - call reject, 107–108
 - HangUP attack, 108–109
 - Hold (QUELCH) attack, 109–110
 - Registration Reject, 106–107
 - in RTP attack
 - message flooding, 88–89
 - RTCP Bye, 89–91
 - in SIP attack
 - via BYE message, 42–43
 - via REGISTER, 44
 - via un-register, 44–45

- dpkt library, installing, 84, 163
- dsniff (Linux), 163
- DTMF tool, 137–138
- duplicate error message, 65–66

E

- E.164 alias
 - audit program, 192–193
 - availability, 63–64
 - for H.323 endpoint, 14, 63–65
 - for H.323 protocol, 54–55
 - enumeration, 65–66
- E.164 hopping attacks, for H.323 protocol, 66–67
- eavesdropping
 - anonymous, 146–148
 - securing SIP session information from, 180
 - with Vonage, 157–161
- eavesdropping of RTP
 - active, 82–87
 - audio insertion, 82–86
 - audio replacement, 87
 - passive, 76–82
 - Cain & Abel for man-in-the-middle attacks, 78–80
 - man-in-the-middle attack, 76–77
 - with Vonage, 157–161
 - with Wireshark, 80–82

- eBay, 151
- Ekiga, 4, 52
- eNapkin, 127
- encryption
 - in SIP, 29–31
 - with S/MIME, 30–31
 - with TLS, 29–30
 - in Skype, 173
 - symmetric, for H.323 protocol, 52–53
 - in VoIP, 15
- endpoint, 11
 - spoofing for H.323 protocol, 63–65
- enumeration
 - E.164 alias for H.323 protocol, 65–66
 - MAC addresses on subnet, 159
 - SIP devices on network, 25–26
 - username, 65–66
 - for H.323 protocol, 56–57
 - in IAX, 96–97
 - in SIP attack, 31–33
- enumIAX tool, 96–97
- error messages, enumerating SIP usernames with, 31–32
- etherchange, 63
- Ethernet connection, phones
 - with, 11
- expiration value, in REGISTER method (SIP), and un-register process, 44–45
- Extensible Messaging and Presence Protocol (XMPP), for Google Talk, 170
- extensions.conf* file, 4, 137
 - backup, 132
 - and caller ID spoofing, 145
 - information from VoIPJet, 143
 - for Zfone, 185

F

- firewalls, 186–187
- From field (SIP), 21
- FTP (File Transfer Protocol),
 - security issues, 121
- fuzzing SIP, 45–47

G

- Garbutt, Alex, 84, 163
- GCF (Gatekeeper Confirmation)
 - packet, 128
- GetIf, 119
- Google Talk, 13, 170–171
 - lightweight SPIT with, 150–151
- government data protection standards, compliance with, 9
- GRQ (Gatekeeper Request)
 - packet, 128

H

- H.225 protocol, 49
 - Denial of Service via
 - nonStandardMessage, 71–72
 - for H.323 authentication, 58
 - audit program, 190
 - hex information example of
 - registration request packet, 62
 - Registration Admission Status (RAS), 55–56
 - Registration Reject packets, 68–69
- H.239 protocol, 49
- H.245 protocol, 49
- H.323 client, 4
 - configuring, 5
- H.323 gatekeeper, 11, 50
 - redirecting, 127–128
 - registering with, 51–52
 - SBC interaction with, 187
- H.323 gateway, 11, 50
- H.323 protocol, 9, 10, 19, 49
 - default authentication type, 13
 - E.164 alias for endpoint, 14
 - network reliability, 72
 - ports, 50
 - security attacks, 55–72
 - Denial of Service via H.225
 - nonStandardMessage, 71–72
 - Denial of Service via host unreachable packets, 70–71

- Denial of Service via NTP, 67–68
 - Denial of Service via UDP, 68–69
 - E.164 alias enumeration, 65–66
 - E.164 hopping attacks, 66–67
 - endpoint spoofing, 63–65
 - password retrieval, 58–59
 - replay attack, 60–63
 - username enumeration, 56–57
 - security basics, 50–55
 - authorization, 54–55
 - enumeration, 50–52
 - password hashing, 53–54
 - public key, 54
 - symmetric encryption, 52–53
 - VoIP deployments with devices, 12
 - H.323.conf* file, 4
 - H.323-ID, Wireshark for sniffing, 56–57
 - H.450 protocol, 49
 - H.460 protocol, 49
 - handsets, 173–174
 - HangUP attack, in IAX, 108–109
 - hard phones, 11, 20, 115–120
 - audit program, 196
 - cable connections, and network vulnerability, 114–115
 - call handling for, 120
 - compromising configuration file, 116–117
 - SNMP weaknesses, 119–120
 - uploading malicious configuration file, 117–119
 - vulnerability to DoS attack, 71
 - header in packet, 9
 - Hewlett-Packard, 67
 - HMAC-SHA1, secure RTP with, 182–183
 - Hold (QUELCH) attack, in IAX, 109–110
 - home VoIP services, 9, 153–154
 - host unreachable packets, Denial of Service via, 70–71
 - HTTP protocol
 - as cleartext protocol, 116
 - and SIP, 20, 180
 - hub, sniffing on, 76
 - Hunt, 83
- I**
- IAX (Inter-Asterisk eXchange) protocol, 9, 11, 93
 - audit program, 192
 - authentication, 94–96
 - audit program, 191
 - default type, 13
 - control frame sequencing predictability, 103
 - VoIP deployments with devices, 12
 - IAX client, 4
 - configuring, 5–6
 - IAX security attacks, 96–110
 - active dictionary attack, 100–102
 - Denial of Service, 106–110
 - call reject, 107–108
 - HangUP attack, 108–109
 - Hold (QUELCH) attack, 109–110
 - Registration Reject, 106–107
 - man-in-the-middle attack, 102–103
 - MD5-to-plaintext downgrade attack, 103–105
 - offline dictionary attack, 97–100
 - username enumeration, 96–97
 - IAXAuthJack, 104–105
 - IAX.Brute tool, 99
 - iaxComm, for caller ID spoofing, 140–142
 - iax.conf* file, 4
 - backup, 132
 - IAXHangup.py tool, 108–109
 - ICMP, Host Unreachable packets to execute DoS attack, 70
 - infrastructure VoIP attacks, 113
 - Avaya Call Center, 120–123
 - Cisco CallManager, 120–123

infrastructure VoIP attacks,
continued
 hard phones, 115–120
 compromising configuration
 file, 116–117
 SNMP weaknesses, 119–120
 uploading malicious configu-
 ration file, 117–119
 Modular Messaging, 123–126
 Nessus for discovering
 vulnerable services, 123
 Nikto to scan web management
 interfaces, 122–123
 Nmap to scan VoIP devices,
 121–122
 server impersonation, 126–128
 redirecting H.323
 gatekeepers, 127–128
 spoofing SIP proxies and
 registrars, 126–127
 vendor-specific sniffing, 114–115
 injection attacks, 82, 83–86
 integrity protection, IAX protocol
 and, 103
 Inter-Asterisk eXchange (IAX)
 protocol. *See* IAX (Inter-
 Asterisk eXchange)
 protocol
 internal network, caller ID spoof-
 ing, with VoIP and SIP,
 144–146
 INVITE method (SIP), 20, 23–25,
 126–127
 audit program and, 190
 IP (Internet Protocol), for voice
 communications, 8
 IP PBX, 11
 IPSec, 15
 ITU-T protocols, 49
 IVR services for users, from Asterisk
 PBX, 136

J

Jabber open source group, 170
 jitter, 73
 Junk Fax Prevention Act of 2005, 133

K

key distribution method,
 in SRTP, 183
 Kismet, 175

L

lab setup, 3–6, 132
 Lackey, Zane, 84, 101, 104, 108, 163
 landline home phone
 Microsoft Live Messenger
 calls to, 172
 security, vs. VoIP security, 154
 Yahoo! Messenger calls to, 168
 language, hard phone
 configuration, 118
 LDAP (Lightweight Directory
 Access Protocol), audit
 program, 191
 libSRTP, 183
 Linux, packages for RTPInject, 84
 Live Messenger (Microsoft), 13, 172
 lockout, reducing risk, 98
 logging
 audit program, 196
 security issues, 121
 Lynksys, 173

M

MAC (Machine Access Control)
 addresses
 in E.164 alias, 14
 enumerating on subnet, 159
 filtering, 55
 for wireless access point, 63
 man-in-the-middle attack
 and, 76
 management methods, audit
 program, 195
 man-in-the-middle attacks
 in IAX, 102–103
 in RTP, 76–77
 Cain & Abel for, 78–80
 in SIP, 36, 38
 MD5 authentication, in IAX, 94–96

- MD5 hash
 - ASN.1-encoded buffer for, 58
 - audit program, 190
 - brute-force attacks, 166
 - from SIP User Agent, 28
 - SIP User Agent creation of
 - response value, 33
 - MD5-to-plaintext downgrade attack,
 - in IAX, 103–105
 - media encryption, audit
 - program, 191
 - message flooding, for RTP Denial
 - of Service attack, 88–89
 - messages, in SIP, 21–22
 - Microsoft Live Messenger, 13, 172
 - Modular Messaging (Avaya),
 - 123–126
 - preventing authentication
 - attacks, 125
 - Montoro, Massimiliano, 78, 159
- N**
- NAT (Network Address
 - Translation), 186
 - national destination code (NDC),
 - in E.164 alias, 14
 - National Do Not Call Registry, 147
 - Nemesis, 61
 - executing DoS attack, 69, 70
 - for RTP packet creation, 88–89,
 - 90–91
 - for UDP packet generation, 68
 - Nessus, 121
 - for discovering vulnerable
 - services, 123
 - Net2Phone, 153
 - Netgear, 173
 - Network Address Translation
 - (NAT), 186
 - network sniffing
 - enumerating SIP usernames
 - with, 32–33
 - and IAX registration traffic, 105
 - vendor-specific VoIP, 114–115
 - Network Time Protocol (NTP),
 - Denial of Service via,
 - 67–68
 - Nikto, 121
 - to scan web management
 - interfaces, 122–123
 - nmap command, 25, 50–51
 - to scan VoIP devices, 121–122
 - nonce (challenge), 27, 28, 29
 - nonStandardMessage, Denial of
 - Service via, 71–72
 - NTP (Network Time Protocol),
 - Denial of Service via,
 - 67–68
- O**
- offline dictionary attack, 33, 35, 58,
 - 166, 180
 - in IAX, 97–100
 - Open Ser TLS, implementation
 - steps, 181
 - open STATE for IP address, and
 - SIP device, 26
 - OpenSSH, security issues, 121
 - OpenSSL, security issues, 121
 - OPTIONS method (SIP), 21
 - OSI model, with VoIP, 10
 - outbound dialing, controls for, 66
 - Outlook plug-in, in Modular
 - Messaging, security
 - issues, 124
- P**
- packets, 9
 - generation tool, 61
 - passive dictionary attack, 99
 - passive eavesdropping of RTP,
 - 76–82
 - man-in-the-middle attacks,
 - 76–77
 - Cain & Abel for, 78–80
 - with Wireshark, 80–82
 - password verifiers, 95*n*
 - password-equivalent values, 95

- passwords
 - hashing for H.323 protocol, 53–54
 - retrieval
 - in H.323 protocol attack, 58–59
 - in SIP attack, 33–37
 - from Vonage, 166–167
 - for voicemail, 9
 - PayPal, as email phisher target, 151
 - PC-based VoIP solutions, 167–173
 - Google Talk, 13, 170–171
 - lightweight SPIT with, 150–151
 - Microsoft Live Messenger, 13, 172
 - Skype, 13, 153, 173
 - icon to initiate outgoing VoIP calls, 133–135
 - lightweight SPIT with, 150–151
 - SOHO phone solutions, 173–175
 - Yahoo! Messenger, 13
 - audio insertion, 170
 - eavesdropping on, 168–170
 - phishing, 133–137
 - phones. *See* hard phones; soft phones
 - PINs, for hard phones, audit program, 196
 - plaintext authentication, in IAX, 94
 - Polycom, VoIP hard phone, security issues, 115–120
 - port scan, 50
 - Nmap for, 121
 - ports, for VoIP, 186
 - power outage, and VoIP, 153
 - PowerPlay, 4
 - pre-computed attacks, 100–101
 - pre-recorded calls, sending over VoIP, 148–150
 - pre-texting, 140
 - privacy
 - Modular Messaging risks to, 123
 - VoIP security and, 8
 - protocols, for VoIP, 9–11
 - PROTOS project, 46
 - Proxy server for SIP, 20
 - SBC interaction with, 187
 - pypcap library, installing, 84, 163

Q

 - QoS (Quality of Service)
 - RTCP for sending information, 73
 - for SIP, 15
 - quality, of VoIP services, 154
 - QUELCH (Hold) attack, in IAX, 109–110

R

 - RAS (Registration Admission Status), for H.225 protocol, 55–56
 - Real Time Control Protocol (RTCP), 73
 - Real-time Transport Protocol (RTP), 9, 10
 - entropy, audit program, 192
 - receiving phishing calls, 136–137
 - Redirect server, for SIP, 20
 - redirecting
 - calls, 146–147
 - H.323 gatekeepers, 127–128
 - REGAUTH packet, in downgrade attack, 104
 - REGISTER request (SIP), 21
 - audit program, 190
 - for Denial of Service attack, 44
 - Registrar server, for SIP, 20
 - Registration Admission Status (RAS), for H.225 protocol, 55–56
 - Registration Reject attack, in IAX, 106–107
 - registration request (REGREQ) packet, for Asterisk server, 104
 - registration with SIP identified devices, 22–23, 26–27
 - hijacking in SIP attack, 38–41
 - replay attack
 - for H.323 protocol, 60–63
 - MD5 hash vulnerability to, 95

- response packet, from User Agent, 166
- RFC (Request for Comments)
 - 3261 on SIP, 19
 - 3711 on Secure RTP, 181
- RJ-45 connector, phones with, 11
- RSA authentication, in IAX, 94
- RTCP (Real Time Control Protocol), 73
- RTCP Bye, for RTP Denial of Service attack, 89–91
- RTP (Real-time Transport Protocol), 9, 10, 73
 - basics, 73–75
 - entropy, audit program, 192
 - packet exchange, 24
 - payload encryption, 181
 - ports, 186
 - security attacks, 75–91
- RTP security attacks
 - active eavesdropping, 82–87
 - audio insertion, 82–86
 - audio replacement, 87
 - Denial of Service, 88–91
 - message flooding, 88–89
 - RTCP Bye, 89–91
 - passive eavesdropping, 76–82
 - Cain & Abel for man-in-the-middle attacks, 78–80
 - man-in-the-middle attack, 76–77
 - with Wireshark, 80–82
 - voice injection, 162–165
- RTPInject, 84–86, 163, 175

S

- S/MIME (Secure Multipurpose Internet Mail Exchange), SIP with, 30–31
- salted MD5 hashes, 60
- SAS (Short Authentication String), for ZRTP, 184
- SBC (Session Border Controller), 11, 50, 187, 188
- Secure Multipurpose Internet Mail Exchange (S/MIME), SIP with, 30–31
- Secure Real Time Transfer Protocol (SRTP). *See* SRTP (Secure Real Time Transfer Protocol)
- Secure Sockets Layer (SSL). *See* SSL (Secure Sockets Layer)
- securing VoIP, 179–187
 - firewalls, 186
 - Session Border Controller (SBC), 11, 50, 187, 188
 - SIP over SSL/TSL (SIPS), 180–181
 - ZRTP and Zfone, 183–185
- security, landline home phone vs. VoIP, 154
- Security Denial Message, 65–66
- sequence number
 - for RTP, 74
 - in Vonage injection attack, 162–163
- servers
 - Asterisk, 26, 93, 132
 - configuring, 4
 - connecting SIP client to, 142
 - for free calls, 138
 - for IVR services for users, 136
 - man-in-the-middle attack of, 102–103
 - to send pre-recorded messages, 148–150
 - SRTP implementation steps, 183
 - DNS server
 - audit program, 197
 - hard phone configuration, 118
 - lookup by Proxy server, 23
 - impersonation, 126–128
 - redirecting H.323 gatekeepers, 127–128
 - spoofing SIP proxies and registrars, 126–127
 - SIP/IAX/H.323 server
 - concurrent sessions, audit program, 191
 - configuring, 4
 - SIP Proxy, 11
 - spoofing, 126–127
 - SIP server, configuring, 5

- services, on Cisco and Avaya products, 120–121
- Session Border Controller (SBC), 11, 50, 187, 188
- Session Initiation Protocol (SIP). *See* SIP (Session Initiation Protocol)
- setup, for VoIP call, 10
- Short Authentication String (SAS), for ZRTP, 184
- Shulman, Jay, 147
- signature file, in phisher's email client, 135
- Simple Network Management Protocol (SNMP). *See* SNMP (Simple Network Management Protocol)
- Single Sign-On (SSO) token, for Google Talk authentication, 170
- SIP (Session Initiation Protocol), 9, 10
 - authentication, 27–29
 - audit program, 190
 - basics, 19–21
 - buffer overrun attacks, vs. IAX, 94
 - default authentication type, 13
 - encryption, 29–31
 - with S/MIME, 30–31
 - with TLS, 29–30
 - enumerating devices on network, 25–26
 - making VoIP call with, 22–25
 - INVITE request, 23–25
 - registration, 22–23
 - messages, 21–22
 - registration with identified devices, 26–27
 - security attacks, 31–47
 - Denial of Service via BYE message, 42–43
 - Denial of Service via REGISTER, 44
 - Denial of Service via un-register, 44–45
 - fuzzing SIP, 45–47
 - man-in-the-middle attack, 38
 - password retrieval, 33–37
 - registration hijacking, 38–41
 - spoofing proxy servers and registrars, 41
 - tools to perform, 36–37
 - username enumeration, 31–33
 - server configuration, 5
 - VoIP deployments with devices, 12
 - for Vonage, 166
- SIP client, 4
 - for caller ID spoofing, 142–143
 - configuring, 5
- SIP/IAX/H.323 server
 - concurrent sessions, audit program, 191
 - configuring, 4
- SIP over SSL/TSL (SIPS), 180–181
- SIP Proxy servers, 11
 - spoofing, 126–127
- SIP Registrar, 11
 - sip.conf* file, 4
 - backup, 132
 - and caller ID spoofing, 144
 - for Zfone, 184
- SIPS (SIP over SSL/TSL), 180–181
- SIP.Tastic tool, 36, 167, 168
- SiVuS tool, 32, 40
- Skype, 13, 153, 173
 - icon to initiate outgoing VoIP calls, 133–135
 - lightweight SPIT with, 150–151
- SkypeOut, 138
- Sniffer Pro, 61
 - for RTP packet creation, 88
- sniffing network
 - enumerating SIP usernames with, 32–33
 - and IAX registration traffic, 105
 - vendor-specific VoIP, 114–115
- SNMP (Simple Network Management Protocol), 195
 - exploiting weaknesses, 119
 - security issues, 121
- social engineering, 132
- soft phones, 11, 13, 20
 - Zfone and, 187

- SOHO phone solutions, 173–175
- Sox for Linux, 85, 164
- spam attack, 131
- spammer, voicemail from, 147
- SPIT (Spam Over Internet Telephony), 147–151
- spoofing
 - caller ID, 139–146
 - with iaxComm and VoIPJet, 140–142
 - impact, 146
 - on internal network with VoIP and SIP, 144–146
 - from services on websites, 143–144
 - with SIP client, 142–143
 - endpoint for H.323 protocol, 63–65
 - REJECT packet, 107
 - SIP message, 40
 - SIP proxy servers and registrars, 41, 126–127
 - user identity, 39
- SRTP (Secure Real Time Transfer Protocol), 15, 75
 - with HMAC-SHA1, 182–183
 - key distribution method, 183
 - key exchange, audit program, 192
 - media protection with AES cipher, 182
- SSL (Secure Sockets Layer), 15
 - attacks on Google Talk, 170–171
 - audit program, 191
 - audit program for certificates, 197
 - certificates, 121
- SSO (Single Sign-On) token, for Google Talk authentication, 170
- SSRC number
 - for RTP packet replacement, 87
 - in Vonage injection attack, 162–163
- Stunnel, 15
- subnet, enumerating MAC addresses on, 159
- subscriber number (SN), in E.164 alias, 14
- Swift, 136–137
- switches, sniffing on, 76
- symmetric encryption, for H.323 protocol, 52–53
- synchronization, RTCP for, 89
- synchronization source for RTP (SRRC), 74

T

- targeted attack, 146
 - with IAXHangup, 109
 - for testing IAXAuthJack, 105
 - for testing vnak, 102
- telephone. *See* hard phones; soft phones
- telephone audio key tones, conversion to text, 137–138
- telephone infrastructure, attacks, 7
- telnet, security issues, 121
- TFTP (Trivial File Transfer Protocol), as cleartext protocol, 116
- timestamp
 - for audio replacement, 87
 - audit program, 195
 - for H.323 authentication, 67
 - for MD5 hashing, 60
 - for RTP, 74
 - in Vonage injection attack, 162–163
- TLS (Transport Layer Security)
 - for Google Talk authentication, 170
 - for Microsoft Live Messenger, 172
 - for SIP, 29–30, 180
 - Yahoo! Messenger use of, 168
- To field (SIP), 21
- Trammel, Dustin T., 96
- Transport Layer Security (TLS). *See* TLS (Transport Layer Security)
- Trivial File Transfer Protocol (TFTP), as cleartext protocol, 116

U

- UDP (User Datagram Protocol),
 - Denial of Service via, 68–69
- UDP port
 - for IAX, 93
 - for RTP, 73
- unconditional call forwarding, hard phone configuration, 118
- un-register
 - audit program, 191
 - for Denial of Service attack, 44–45
- URI (Uniform Resource Identifier)
 - in E.164 alias, 14
 - for SIP, 22
- User Agents, 13
 - response packet from, 166
 - for SIP, 20
 - registration, 26, 39
- username enumeration
 - for H.323 protocol, 56–57
 - in IAX, 96–97
 - in SIP attack, 31–33
- username retrieval, from Vonage, 166–167

V

- Verizon, 172
- vishing, 133–135
- VLANs
 - audit program, 194
 - for VoIP network, 114
- VMware Player, 4, 26
- vna utility, 36, 101–102
- voice calls, sensitivity, 9
- voice injection, in Vonage, 162–165
- voice network, separating data network from, 15
 - audit program, 194
- voicemail
 - for mobile phones, access to, 146
 - from spammer, 147

- voicemail passcode, 124
- VoIP (Voice over IP), 7. *See also*
 - home VoIP services; infrastructure VoIP attacks
 - auditing for security best practices, 189–197
 - basics, 9–13
 - deployments, 11–13
 - protocols, 9–11
 - commercial solutions, 154–167
 - impact of DoS attack, 106
 - OSI model with, 10
 - PC-based solutions, 167–173
 - Google Talk, 170–171
 - Microsoft Live Messenger, 172
 - Skype, 173
 - SOHO phone solutions, 173–175
 - Yahoo! Messenger, 168–170
- VoIP (Voice over IP) security
 - attack vectors, 15–16
 - basics, 13–15
 - authentication, 13–14
 - authorization, 14
 - availability, 14–15
 - encryption, 15
 - importance, 8–9
 - unconventional threats, 131–132
 - anonymous eavesdropping and call redirection, 146–147
 - caller ID spoofing, 139–146
 - making free calls, 138–139
 - phishing, 133–137
 - receiving calls, 136–137
 - SPIT (Spam Over Internet Telephony), 147–151
- VoIP Security Audit Program (VSAP), 190–197
 - downloading, 190
- VoIPBuster, for free calls, 138
- VoIPJet, 140–142, 150
- VoIPonCD-appliance, 132

Vonage, 153
 security attacks, 154–161
 call eavesdropping, 157–161
 probabilities, 156
 username/password
 retrieval, 166–167
 voice injection, 162–165
VSAP (VoIP Security Audit
 Program), 190–197
 downloading, 190

W

.wav files
 decoding RTP packets to, 78, 80
 RTPInject transcoding of, 85
website services, for caller ID
 spoofing, 143–144
WEP (Wired Equivalent Privacy),
 157, 174–175
Wi-Fi Protected Access (WPA), 157,
 174–175
wildcard attack
 with IAXHangup, 109
 for testing IAXAuthJack, 105
Windows Sound Recorder, 85, 164
Wired Equivalent Privacy (WEP),
 157, 174–175
wireless technology, 16
 attack surface on home
 devices, 156
Wireshark, 33
 to capture RTP packets, 158
 dialedDigits line for destination
 E.164 alias, 65
 for H.225.0 RAS entry, 61
 and MD5 hash with H.225
 packet, 62
 to reassemble RTP packets,
 80–82
 for sniffing H.323-ID, 56–57
 stream analysis, 81
WPA (Wi-Fi Protected Access), 157,
 174–175

X

X-Lite, 4, 5, 26–27
 connecting SIP client to Asterisk
 server, 142
 for free calls, 138
 for targeted attack, 147
 using Zfone with, 184–185
XEP (XMPP Extension
 Protocols), 170
XMPP (Extensible Messaging and
 Presence Protocol), for
 Google Talk, 170

Y

Yahoo! Messenger, 13
 audio insertion, 170
 eavesdropping on, 168–170

Z

Zfone, 183–185
ZRTP, 183–185