

INDEX

A

- AAA (authentication, authorization, and auditing). *See* Diameter Base Protocol
- ACA (Australian Communications Authority), 6
- access
 - enterprise VoIP
 - architecture, 307-311
 - unauthorized access, 58, 76-80
 - exploiting software vulnerabilities, 83
 - SIP authentication dictionary attack, 80-82
- Address Resolution Protocol, 88
- addressing, private, 269-270
- ADSL (Asymmetric Digital Subscriber Line), 31
- Advance Intelligent Network (AIN), 4
- agents, 271
- AIN (Advance Intelligent Network), 4
- ALE (Annual Loss Expectancy), 20
- ALG (Application-Level Gateway), 43
 - analyzing vulnerabilities, 160-162
 - annoyance, 75-76
 - Annual Loss Expectancy (ALE), 20
 - Application-Level Gateway (ALG), 43
 - architecture, 32, 264
 - carrier VoIP networks. *See* carrier VoIP networks
 - enterprise VoIP networks. *See* enterprise VoIP networks
 - IMS, 41
 - network management configuration, 268-269
 - network segmentation, 264-267
 - peer-to-peer IP telephony, 32-34
 - private addressing, 269-270
 - service provider
 - architectures, 39
 - softswitch
 - architecture, 39-40
- asset management, 301
- asterisk IP-PBX
 - architectures, 339
- Asymmetric Digital Subscriber Line (ADSL), 31
- at variable (ZRTP key negotiation), 254
- attacks. *See also* threats defined, 54
 - DoS. *See* DoS attacks
 - telephony services
 - call forwarding, 62
 - caller ID, 62
 - confidentiality, 63
 - emergency services, 64
 - follow-me service, 62
 - lawful intercept, 63
 - location and presence services, 63
 - voicemail, 61
 - vulnerabilities, 129-130
- auditing (Diameter Base Protocol)
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR) command, 279
- proxy agents, 271
- Push-Profile-Answer (PPA) command, 280
- Push-Profile-Request (PPR) command, 280
- redirect agents, 271
- Registration-Termination-Answer (RTA) command, 280

- Registration-
 - Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - SIP, 272-277
 - translation agents, 271
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
 - AUEP (Audit End-Point) message, 96
 - Australian Communications Authority (ACA), 6
 - Australian Network Reliability Framework (NRF), 6
 - authentication
 - Diameter Base Protocol
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR) command, 279
 - proxy agents, 271
 - Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - redirect agents, 271
 - Registration-
 - Termination-Answer (RTA) command, 280
 - Registration-
 - Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - SIP, 272-275, 277
 - translation agents, 271
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
 - auto-dialers, 116
 - availability (PSTN), 55
- B**
- BCE (border control element), 331-332
 - Bellcore, 4
 - business continuity management, 313
- C**
- Cain & Abel,
 - eavesdropping, 86-92
 - call forwarding, 62
 - call manager/agent, 336
 - call managers, 42, 109-110
 - call-flow manipulation, 117-120
 - caller ID, 62
 - spoofing, 102-103
 - calls, diverting, 109-110
 - carrier-grade VoIP
 - architecture, 38
 - components of, 315-317
 - security, 327-328
 - BCE, 331-332
 - developing security requirements, 332-333
 - DOS attacks, 329
 - subscriber device authentication, 328
 - user authentication, 329

- categories
 - CWE. *See* CWE
 - OWASP. *See* OWASP
 - VoIP, 142-143
 - VOIP-01 insufficient verification of data, 144-146
 - VOIP-02 execution flaws, 146
 - VOIP-03
 - string/array/pointer manipulation flaws, 147-149
 - VOIP-04 low resources, 149
 - VOIP-05 low bandwidth, 150
 - VOIP-06 file/resource manipulation flaws, 151-152
 - VOIP-07 password management, 152
 - VOIP-08 permissions and privileges, 153
 - VOIP-09 crypto and randomness, 153-154
 - VOIP-10 authentication and certificate errors, 155-157
 - VOIP-11 error handling, 157-158
 - VOIP-12 homogeneous network, 158
 - VOIP-13 lacking fallback system, 158
 - VOIP-14 physical connection quality and packet collision, 159
- CC (Common Criteria), 24
- CEM (Common Evaluation Methodology), 24
- certification, 23-25
- Chief Information Security Officer (CISO), 21
- Chief Security Officer (CSO), 21
- CIO (chief information officer), 21
- cipher variable (ZRTP key negotiation), 254
- circuit-switched networks. *See* PSTN
- CISO (Chief Information Security Officer), 21
- clients, Diameter, 270
- closed VoIP, 13
- CNI (Critical National Infrastructure), 12, 24
- commands, Diameter
 - Location-Info-Answer (LIA), 279
 - Location-Info-Request (LIR), 279
 - Multimedia-Auth-Request (MAR), 279
 - Push-Profile-Answer (PPA), 280
 - Push-Profile-Request (PPR), 280
 - Registration-Termination-Answer (RTA), 280
 - Registration-Termination-Request (RTR), 279
 - Server-Assignment-Answer (SAA), 278
 - Server-Assignment-Request (SAR), 278
 - User-Authorization-Answer (UAA), 278
 - User-Authorization-Request (UAR), 278
- Common Evaluation Methodology (CEM), 24
- Common Vulnerabilities and Exposures (CVE), 130
- Common Weakness Enumeration. *See* CWE
- compliance, enterprise VoIP architecture, 313-314
- components
 - of carrier-grade VoIP architectures, 315-317
 - of enterprise VoIP, 335-338
- computations, KEMAC, 238-239
- confidentiality, 63
- configuration management, 159-160, 268-269
- control, 160
- converged telco, 319-323
- Critical National Infrastructure (CNI), 12, 24
- Cross-Site Scripting (XSS), 140
- crypto session (CS), 236, 242-243
- crypto session bundle (CSB), 236
- crypto session bundle ID (CSB ID), 236
- cryptography, 134
- CS (crypto session), 236, 242-243
- CSB (crypto session bundle), 236
- CSB ID (crypto session bundle ID), 236
- CSO (Chief Security Officer), 21
- CTO (Chief Technology Officer), 21
- CVE (Common Vulnerabilities and Exposures), 130
- CWE (Common Weakness Enumeration)

- CWE-01 insufficient verification of data, 130-131
 - CWE-02 pointer issues, 131
 - CWE-03 resource management errors, 132
 - CWE-04 race conditions, 132
 - CWE-05 temporary file issues, 133
 - CWE-06 password management, 133
 - CWE-07 permissions, privileges, and ACLs, 133
 - CWE-08 cryptographic errors, 134
 - CWE-09 randomness and predictability, 135
 - CWE-10 authentication errors, 135-136
 - CWE-11 certification issues, 136
 - CWE-12 error handling, 137-138
- D**
- data confidentiality, 18
 - data encryption (SRTP), 219
 - data integrity, 19
 - Data Over Cable Service Interface Specification (DOCSIS), 31
 - data security association, 236
 - Datagram Transport Layer Security (DTLS), 183-186
 - Denial of Service attacks. *See* DoS attacks
 - deployments, VoIP, 12-15
 - development, enterprise VoIP architecture, 311-312
 - DH (Diffie-Hellman) key exchange, 235, 239
 - DHCP, 50
 - Diameter Base Protocol, 270-271
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR) command, 279
 - proxy agents, 271
 - Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - redirect agents, 271
 - Registration-Termination-Answer (RTA) command, 280
 - Registration-Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - SIP, 272-277
 - translation agents, 271
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
 - Diffie-Hellman (DH) key exchange, 235, 239
 - distributed architecture, 342
 - diverting calls, 109-110
 - DNS, 50
 - DOCSIS (Data Over Cable Service Interface Specification), 31
 - DoS attacks, 64-65, 70-71
 - carrier-grade VoIP architecture, 329
 - malformed packets, 71
 - service disruption, 59-61
 - SIP flooding attacks, 72-73
 - SIP signaling loop attacks, 73-74
 - target layers, 65-69
 - ZRTP, 258
 - DTLS (Datagram Transport Layer Security), 183-186
 - DTMF (Dual Tone Multi Frequency), 153, 259-260
- E**
- early media, 227
 - eavesdropping, 84-85
 - with Cain & Abel, 86—92
 - with Ethereal/Wireshark, 85-86
 - real-time eavesdropping by manipulating MGCP, 94-100
 - with VLAN hopping, 93-94
 - eavesdropping and traffic analysis, 57
 - emergency services, 64
 - End-User License Agreements (EULAs), 15
 - enterprise PBX architectures
 - asterisk IP-PBX architectures, 339
 - hybrid IP-PBX architectures, 338-339

enterprise VoIP architecture,
12, 36-38
asset management, 301
business continuity
management, 313
compliance, 313-314
components of, 335-338
external parties, 299-300
information systems
acquisition,
development, and
maintenance, 311-312
network topologies,
338-343
security, 343-344
access control, 307-311
equipment
security, 302-304
incident
management, 312-313
operations
management, 304-307
physical and
environmental
security, 301-302
policies, 298-299
ENUM, 51
environmental
security, 301-302
equipment security, 302-304
Ethereal, 85-86
EULAs (End-User License
Agreements), 15
exploiting software
vulnerabilities, 83
external parties, 299-300

F

FIPS 140, 24
firewalls, 280-282
five nines (99.999), 55
follow-me service, 62

fraud, 58, 113-114
call-flow
manipulation, 117-120
managing, 123-125
phishing, 120-123
types of, 115-116
in VoIP, 116-117
FUD (Fear, Uncertainty,
and Doubt), 3

G-H

General Packet Radio Service
(GPRS), 31
GIAC (Global Information
Assurance
Certification), 23

H.235, 194-196
H.235.1 baseline security
profile, 196-198
H.235.2 signature security
profile, 200-201
H.235.3 hybrid security
profile, 201-203
H.235.4 directed and
selected call routing
security, 203-204
H.235.5 framework for
secure authentication
in RAS using weak
shared secrets, 204-205
H.235.6 voice encryption
profile with native
H.235/H.245 key
management, 205-207
H.235.7 usage of MIKEY
key management
protocol for the SRTP
within H.235, 207-209
H.235.8 key exchange
for SRTP using
secure signaling
channels, 210-211

H.235.9 security
gateway support for
H.323, 211-213
limitations, 214
strengths, 213
H.323, 46, 193
hash variable (ZRTP key
negotiation), 254
hmackeyi/r variable (ZRTP
key negotiation), 256
human behavior, 162-163
hvi/r variable (ZRTP key
negotiation), 254
hybrid IP-PBX architectures,
338-339

I

I-VSP (Internet based Voice
Service Provider),
319, 325-326
identification, 160
identifying threats, 54
IDS (intrusion detection
systems), 289-294
IEEE 802.1x, 343
IETF drafts, 56
impersonating call
managers, 109-110
implosion, avoiding, 233
IMS (Internet Protocol
Multimedia
Subsystem), 1,
13, 30, 41
information systems acqui-
sition, 311-312
integrated keying, 232
integrity, 224
interactive voice response
(IVR) system, 337
interconnection standards, 30
International Information
Systems Security
Certification
Consortium, 23

- International Packet Communications Consortium (IPCC), 39
 - Internet, IP and, 11
 - Internet Protocol Multimedia Subsystem (IMS), 1, 13, 30, 41
 - Internet Protocol. *See* IP
 - Internet telephony, 12
 - Internet-based Voice Service Provider (I-VSP), 319, 325-326
 - Internet-based VoIP deployments, 12
 - intrusion detection systems (IDS), 289-294
 - IP (Internet Protocol), 1
 - IMS (Internet Protocol Multimedia Subsystem), 1, 13, 30, 41
 - Internet and, 11
 - IP-PBX, 336
 - IPv4, 50
 - IPv6, 50
 - VoIP and, 9-12
 - IP-PBX, 336
 - IPCC (International Packet Communications Consortium), 39
 - IPsec, 190-192
 - IPv4, 50
 - IPv6, 50
 - ISO 17799/27001, 297
 - ISP-VSP (ISP-based voice service provider), 319, 323-324
 - ISUP, 46
 - IT, VoIP as part of, 21-22
 - IVR (interactive voice response) system, 337
- J-K**
- KEMAC, 238-239
 - key derivation (SRTP), 225-226
 - key management
 - implosion avoidance, 233
 - integrated keying, 232
 - MIKEY (Multimedia Internet KEYing)
 - combining with SIP, 244-247
 - crypto session ID, 236
 - CS (crypto session), 236, 242-243
 - CSB (crypto session bundle), 236
 - CSB ID (crypto session bundle ID), 236
 - data security
 - association, 236
 - data security protocols, 236
 - DH (Diffie-Hellman) key exchange, 235, 239
 - message attributes, 237
 - message
 - creation, 240-242
 - message exchange, 237, 240
 - overview, 234-235
 - PKE (public key encryption), 235
 - PSK (pre-shared secret key), 235
 - sessions, establishing, 236-240
 - TEK (traffic-encrypting key), 236
 - TGK (TEK-generation key), 236
 - native key exchange, 232
 - overview, 231-233
 - RFC 4046 (MSEC Group Key Management Architecture), 231
 - session establishment delay, 233
 - SRTP, 224, 247-250
 - ZRTP
 - DoS, 258
 - DTMF (Dual Tone Multi Frequency) disclosure, 259-260
 - key negotiation, 251-256
 - man-in-the-middle attacks, 258
 - overview, 251
 - Zfone, 256-257
 - key variable (ZRTP key negotiation), 254
 - KISS (Keep It Simple, Stupid), 18
- L**
- lawful intercept, 63
 - LIA (Location-Info-Answer) command, 279
 - LIR (Location-Info-Request) command, 279
 - location and presence services, 63
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - logging and auditing, 344
- M**
- maintenance, enterprise VoIP architecture, 311-312
 - malformed packet denial of service attacks, 71
 - man-in-the-middle attacks, 258

- MAR (Multimedia-Auth-Request)
 - command, 279
 - masquerading, 58, 101-102
 - caller ID spoofing, 102-103
 - impersonating call
 - managers and diverting all calls, 109-110
 - listing of attacks, 110-112
 - presence hijacking, 103-108
 - Master Key Identifier (MKI), 220
 - media
 - early media, 227
 - media gateways, 43
 - carrier-grade VoIP architectures, 316
 - enterprise VoIP, 336
 - Media Gateway Control Protocol (MGCP), 48, 94-100, 214-216
 - media servers, 43
 - media transport protocols, 31
 - RTCP, 49
 - RTP, 49
 - RTSP, 47
 - SRTCP, 227
 - SRTP, 218-228
 - key derivation, 225-226
 - key management, 224
 - limitations of, 228
 - packets, 222
 - strengths, 228
 - user authentication and integrity, 224
 - Media Gateway Control Protocol. *See* MGCP
 - media gateway, 43
 - carrier-grade VoIP architectures, 316
 - enterprise VoIP, 336
 - Media Gateway Control Protocol (MGCP), 48, 94-100, 214-216
 - media servers, 43
 - media transport protocols, 31
 - RTCP, 49
 - RTP, 49
 - RTSP, 47
 - messages
 - authentication (SRTP), 220
 - Diameter message
 - format, 271-272
 - MIKEY
 - attributes, 237
 - creating, 240-242
 - message
 - exchange, 237, 240
 - MGCP (Media Gateway Control Protocol), 48, 214-215
 - limitations, 216
 - protecting against attacks, 215
 - real-time eavesdropping, 94-100
 - strengths, 216
 - MIKEY (Multimedia Internet KEYing)
 - combining with SIP, 244-247
 - CS (crypto session), 236, 242-243
 - CSB (crypto session bundle), 236
 - CSB ID (crypto session bundle ID), 236
 - data security
 - association, 236
 - data security protocols, 236
 - DH (Diffie-Hellman) key
 - exchange, 235, 239
 - H.235.7, 207-209
 - message attributes, 237
 - message creation, 240-242
 - message exchange, 237, 240
 - overview, 234-235
 - PKE (public key encryption), 235
 - PSK (pre-shared secret key), 235
 - sessions, establishing, 236-240
 - TEK (traffic-encrypting key), 236
 - TGK (TEK-generation key), 236
 - MKI (Master Key Identifier), 220
 - mobility, peer-to-peer networks, 33
 - MPLS (Multi Protocol Label Switching), 10, 342
 - MSEC Group Key Management Architecture (RFC 4046), 231
 - Multi Protocol Label Switching (MPLS), 10, 342
 - Multimedia Internet KEYing. *See* MIKEY
 - Multimedia-Auth-Request (MAR) command, 279
- ## N
- NAPT (Network and Port Address Translation), 280
 - NAT, 280-282
 - national security and emergency preparedness (NS/EP), 6
 - National Security Telecommunications Advisory Committee (NSTAC), 6

- native key exchange, 232
 - Network and Port
 - Address Translation (NAPT), 280
 - network components
 - call managers, 42
 - management
 - configuration, 268-269
 - media servers/gateways, 43
 - session border elements, 43
 - signaling servers/gateways, 42
 - terminals, 41-42
 - network reliability, 6
 - network security controls
 - AAA (authentication, authorization, and auditing), 271
 - architectural considerations
 - network management
 - configuration, 268-269
 - network
 - segmentation, 264-267
 - private
 - addressing, 269-270
 - Diameter Base Protocol
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR)
 - command, 279
 - proxy agents, 271
 - Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - redirect agents, 271
 - Registration-Termination-Answer (RTA) command, 280
 - Registration-Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA)
 - command, 278
 - Server-Assignment-Request (SAR)
 - command, 278
 - SIP, 272-277
 - translation agents, 271
 - User-Authorization-Answer (UAA)
 - command, 278
 - User-Authorization-Request (UAR)
 - command, 278
 - firewalls, 280-282
 - IDS (intrusion detection systems), 289-294
 - NAT, 280-282
 - overview, 263-264
 - private addressing, 269-270
 - SBCs (Session Border Controllers)
 - call flow, 284
 - capabilities, 285-287
 - configuration, 284
 - limitations, 287-288
 - network placement, 282-284
 - network segmentation, 264-267, 342
 - network topologies
 - converged telco, 319-323
 - enterprise VoIP, 338-343
 - I-VSP, 319, 325-326
 - ISP-based voice service provider (ISP-VSP), 319, 323-324
 - NGN (Next Generation Network), 1
 - NIST SP800-58, 297
 - NRF (Australian Network Reliability Framework), 6
 - NS/EP (national security and emergency preparedness), 6
 - NSTAC (National Security Telecommunications Advisory Committee), 6
- O**
- Open Web Application Security Project. *See* OWASP
 - operations management, 304-307
 - other_secretIDi/r variable (Z RTP key negotiation), 255
 - Oulu University Secure Programming Group (OUSPG), 128
 - OUSPG (Oulu University Secure Programming Group), 128
 - OWASP (Open Web Application Security Project), 139
 - OWASP-01 unvalidated input parameters, 139
 - OWASP-02 Cross-Site Scripting (XSS) flaws, 140
 - OWASP-03 injection flaws, 140
 - OWASP-04 buffer overflows, 140
 - OWASP-05 denial of service (DoS), 140

- OWASP-06 broken access control, 141
 - OWASP-07 insecure storage, 141
 - OWASP-08 broken authentication and session management, 141
 - OWASP-09 improper error handling, 142
 - OWASP-10 insurance configuration management, 142
- P**
- PacketCable architecture, 324-325
 - packets, malformed packet denial of service attacks, 71
 - Panama telecommunications, 7
 - PBX projected shipments from enterprise networks, 340
 - peer-to-peer IP telephony, 32-34
 - phishing, 120-123
 - physical security, 301-302
 - PKE (public key encryption), 235
 - PPA (Push-Profile-Answer) command, 280
 - PPR (Push-Profile-Request (PPR) command, 280
 - pre-paid calling cards, 116
 - pre-shared secret key (PSK), 235
 - presence hijacking, 103-108
 - private addressing, 269-270
 - protection mechanisms, 343 signaling messages. *See* signaling protection mechanisms
 - SIP protection mechanisms, 166-176
 - protocols
 - Diameter Base Protocol, 270-271
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR) command, 279
 - proxy agents, 271
 - Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - redirect agents, 271
 - Registration-Termination-Answer (RTA) command, 280
 - Registration-Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - SIP, 272-277
 - translation agents, 271
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
 - MIKEY (Multimedia Internet KEYing) combining with SIP, 244-247
 - CS (crypto session), 236, 242-243
 - CSB (crypto session bundle), 236
 - CSB ID (crypto session bundle ID), 236
 - data security association, 236
 - data security protocols, 236
 - DH (Diffie-Hellman) key exchange, 235, 239
 - message attributes, 237
 - message creation, 240-242
 - message exchange, 237, 240
 - overview, 234-235
 - PKE (public key encryption), 235
 - PSK (pre-shared secret key), 235
 - sessions, establishing, 236-240
 - TEK (traffic-encrypting key), 236
 - TGK (TEK-generation key), 236
 - NAPT (Network and Port Address Translation), 280
 - NAT, 280-282
 - SRTP Security Descriptions, 247-250

- ZRTP
 DoS, 258
 DTMF (Dual Tone Multi Frequency) disclosure, 259-260
 key negotiation, 251-256
 man-in-the-middle attacks, 258
 overview, 251
 Zfone, 256-257
 proxy agents, 271
 PSK (pre-shared secret key), 235
 PSTN (Public Switch Telephone Network), 1, 4-5
 availability, 55
 overview, 7-9
 public key encryption (PKE), 235
 Public Switch Telephone Network. *See* PSTN
 Push-Profile-Answer (PPA) command, 280
 Push-Profile-Request (PPR) command, 280
 pvi/r variable (ZRTP key negotiation), 254
- Q-R**
 Q.931, 45
 quad play, 1
 RAT (Robust Audio Tool), 100
 real-time eavesdropping by manipulating MGCP, 94-100
 Real-time Streaming Protocol (RTSP), 47
 Real-time Transport Control Protocol (RTCP), 49, 218
 Real-time Transport Protocol (RTP), 49, 217
 redirect agents, 271
 Registration-Termination-Answer (RTA) command, 280
 Registration-Termination-Request (RTR) command, 279
 regulatory requirements, 314
 relay agents, 271
 remote sites (MPLS), 342
 RFC 4046 (MSEC Group Key Management Architecture), 231
 risk analysis, 18-20
 Robust Audio Tool (RAT), 100
 rs1IDi/r variable (ZRTP key negotiation), 255
 rs2IDi/r variable (ZRTP key negotiation), 255
 RSVP, 51
 RTA (Registration-Termination-Answer) command, 280
 RTCP (Real-time Transport Control Protocol), 49, 218
 RTP (Real-time Transport Protocol), 49, 217
 RTR (Registration-Termination-Request) command, 279
 RTSP (Real-time Streaming Protocol), 47
- S**
 S/MIME (Secure/Multipurpose Internet Mail Extensions) limitations, 190
 SIP and, 186-189
 strengths, 190
 SAA (Server-Assignment-Answer) command, 278
 SAR (Server-Assignment-Request) command, 278
 SAS variable (ZRTP key negotiation), 254
 SBCs (Session Border Controllers) call flow, 284
 capabilities, 285-287
 carrier-grade VoIP architectures, 316
 configuration, 284
 limitations, 287-288
 network placement, 282-284
 SCP (service control point), 317
 SCTP (Stream Control Transmission Protocol), 50
 SDP (Session Description Protocol), 48
 Secure Real Time Protocol. *See* SRTP
 Secure/Multipurpose Internet Mail Extensions (S/MIME) limitations, 190
 SIP and, 186-189
 strengths, 190
 security. *See also* key management
 AAA (authentication, authorization, and auditing), 271
 architectural considerations
 network management configuration, 268-269
 network segmentation, 264-267

- private addressing, 269-270
- carrier-grade VoIP
 - architecture, 327-328
 - BCE, 331-332
 - developing security requirements, 332-333
 - DOS attacks, 329
 - subscriber device authentication, 328
 - user authentication, 329
- certifications, 23-25
- challenges in VoIP security, 15-17
- Diameter Base Protocol
 - Diameter clients, 270
 - Diameter servers, 270
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - message format, 271-272
 - Multimedia-Auth-Request (MAR) command, 279
 - proxy agents, 271
 - Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - redirect agents, 271
 - Registration-Termination-Answer (RTA) command, 280
 - Registration-Termination-Request (RTR) command, 279
 - relay agents, 271
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - SIP, 272-277
 - translation agents, 271
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
- enterprise VoIP, 343-344
 - access control, 307-311
 - business continuity management, 313
 - compliance, 313-314
 - equipment security, 302-304
 - information systems acquisition, development, and maintenance, 311-312
 - operations management, 304-307
 - physical and environmental security, 301-302
 - security incident management, 312-313
 - security organization, 21-22
 - security policies, 298-299
 - firewalls, 280-282
 - IDS (intrusion detection systems), 289-294
 - NAT, 280-282
 - overview, 263-264
 - protection mechanisms, 343
 - SBCs (Session Border Controllers) call flow, 284 capabilities, 285-287 configuration, 284 limitations, 287-288 network placement, 282-284 vulnerabilities, 129-130
 - security incident management, 312-313
 - segmented networks, 264-267
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - servers, Diameter, 270
 - service disruption and annoyance, 57-61
 - service provider architectures, 39
 - Service Switching Point (SSP), 5, 317
 - Session Border Controllers. *See* SBCs
 - session border elements, 43
 - Session Description Protocol (SDP), 48
 - session establishment delay, 233
 - Session Initiation Protocol. *See* SIP
 - Signaling System #7 (SS7), 45
 - SigComp (Signaling Compression), 51
 - Signal Transfer Point (STP), 5
 - signaling and media confidentiality, 344
 - signaling gateways, 42
 - carrier-grade VoIP architectures, 316
 - enterprise VoIP, 336

- signaling messages, 165
 - DTLS (Datagram Transport Layer Security), 183-186
- H.235, 194-196
 - H.235.1 baseline security profile, 196-198
 - H.235.2 signature security profile, 200-201
 - H.235.3 hybrid security profile, 201-203
 - H.235.4 directed and selected call routing security, 203-204
 - H.235.5 framework for secure authentication in RAS using weak shared secrets, 204-205
 - H.235.6 voice encryptiton profile with native H.235/H.245 key management, 205-207
 - H.235.7 usage of MIKEY key management protocol for the SRTP within H.235, 207-209
 - H.235.8 key exchange for SRTP using secure signaling channels, 210-211
 - H.235.9 security gateway support for H.323, 211-213
 - limitations, 214
 - strenths, 213
- H.323, 193
- IPsec, 190-192
- MGCP (Media Gateway Control Protocol), 214-216
 - H.235.9 security gateway support for H.323, 211-213
 - limitations, 214
 - strengths, 213
- H.323, 193
- IPsec, 190-192
- MGCP (Media Gateway Control Protocol), 214-215
 - limitations, 216
 - protecting against attacks, 215
 - strengths, 216
- S/MIME, 186, 189-190
- TLS. *See* TLS
- signaling protocols, 30, 44
 - H.323, 46
 - MGCP, 48
 - Q.931, 45
 - SDP, 48
 - Sigtran, 45
 - SIP, 47-48
 - SS7, 45
- signaling servers, 42
- sigsIDi/r variable (ZRTP key negotiation), 255
- Sigtran, 14, 45
- Simple Network Management Protocol (SNMP), 40
- SIP (Session Initiation Protocol), 47-48
 - authentication dictionary attack, 80-82
 - Diameter, 272-277
 - Location-Info-Answer (LIA) command, 279
 - Location-Info-Request (LIR) command, 279
 - Multimedia-Auth-Request (MAR) command, 279
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
 - limitations, 190
 - SIP and, 186-189
 - strengths, 190
- SIP protection mechanisms, 166-176
- TLS (Transport Layer Security), 176-177
 - limitations, 182
 - SIP and, 178-181
 - strengths, 182
- signaling protection mechanisms, 165
- DTLS, 183-185
- H.235, 194-196
 - H.235.1 baseline security profile, 196-198
 - H.235.2 signature security profile, 200-201
 - H.235.3 hybrid security profile, 201-203
 - H.235.4 directed and selected call routing security, 203-204
 - H.235.5 framework for secure authentication in RAS using weak shared secrets, 204-205
 - H.235.6 voice encryption profile with native H.235/H.245 key management, 205-207
 - H.235.7 usage of the MIKEY key management protocol for the SRTP within H.235, 207-209
 - H.235.8 key exchange for SRTP using secure signaling channels, 210-211

- Push-Profile-Answer (PPA) command, 280
 - Push-Profile-Request (PPR) command, 280
 - Registration-
 - Termination-Answer (RTA) command, 280
 - Registration-
 - Termination-Request (RTR) command, 279
 - Server-Assignment-Answer (SAA) command, 278
 - Server-Assignment-Request (SAR) command, 278
 - User-Authorization-Answer (UAA) command, 278
 - User-Authorization-Request (UAR) command, 278
 - flooding attacks, 72-73
 - MIKEY, 244-247
 - protection mechanisms, 166-176
 - signaling loop attacks, 73-74
 - S/MIME and, 186-189
 - TLS (Transport Layer Security) and, 178-181
 - Skype, 34-35
 - SNMP (Simple Network Management Protocol), 40
 - softswitch architecture, 39-40, 316
 - SPIT (spam for/over Internet telephony), 75
 - SRTCP, 227
 - SRTP (Secure Real Time Protocol), 217-228
 - key derivation, 225-226
 - key management, 224
 - limitations of, 228
 - overview, 247
 - packets, 222
 - Security Descriptions, 247-250
 - strengths of, 228
 - user authentication and integrity, 224
 - srtplevel/r variable (ZRTP key negotiation), 255
 - srtpsalt/r variable (ZRTP key negotiation), 255
 - srtpsid/r variable (ZRTP key negotiation), 255
 - SS7 (Signaling System #7), 45
 - SSP (Service Switching Point), 5, 317
 - standards
 - enterprise VoIP architecture, 314
 - interconnection, 30
 - status, 160
 - STP (Signal Transfer Point), 5, 317
 - Stream Control Transmission Protocol (SCTP), 50
 - subscriber device authentication, 328
 - subscribers, 31
 - subscription fraud, 115
 - superimposed fraud, 115
 - svi/r variable (ZRTP key negotiation), 254
- T**
- target layers, 65-69
 - TCP (Transport Control Protocol), 10
 - TDM (Time Division Multiplexing), 29
 - TEK (traffic-encrypting key), 236
 - TEK-generation key (TGK), 236
 - telecommunications
 - network reliability, 6
 - VoIP and, 4-7
 - Telecommunications Industry Association (TIA), 23
 - telephony services
 - attacks related to call forwarding, 62
 - caller ID, 62
 - confidentiality, 63
 - emergency services, 64
 - follow-me service, 62
 - lawful intercept, 63
 - location and presence services, 63
 - voicemail, 61
 - overview, 16
 - terminals, 41-42
 - TGK (TEK-generation key), 236
 - threats, 19, 56. *See also* attacks
 - annoyance, 75-76
 - defined, 53-54
 - eavesdropping, 57, 84-85
 - with Cain & Abel, 86-92
 - with Ethereal/Wireshark, 85-86
 - real-time eavesdropping by manipulating MGCP, 94-100
 - with VLAN hopping, 93-94
 - fraud, 58, 113-114
 - call-flow manipulation, 117-120
 - managing, 123-125
 - phishing, 120-123
 - types of, 115-116
 - in VoIP, 116-117
 - identifying, 54
 - masquerading, 101-102
 - caller ID spoofing, 102-103

- impersonating call managers and diverting all calls, 109-110
 - listing of attacks, 110-112
 - presence
 - hijacking, 103-108
 - masquerading and impersonation, 58
 - service disruption and annoyance, 57-61
 - unauthorized access, 58, 76-80
 - exploiting software vulnerabilities, 83
 - SIP authentication
 - dictionary attack, 80-82
 - TIA (Telecommunications Industry Association), 23
 - Time Division Multiplexing (TDM), 29
 - TLS (Transport Layer Security), 50, 176
 - Handshake Protocol, 177
 - limitations, 182
 - Record Protocol, 176
 - SIP and, 178-181
 - strengths, 182
 - traffic-encrypting key (TEK), 236
 - traffic policy
 - enforcement, 342
 - transcoding, 284
 - translation agents, 271
 - Transport Control Protocol (TCP), 10
 - Transport Layer Security.
See TLS
 - triple play, 1
 - trusted elements, 195
- U**
- UAA (User-
Authorization-Answer)
command, 278
 - UAR (User-
Authorization-Request)
command, 278
 - UDP (User Datagram
Protocol), 10
 - unauthorized access,
58, 76-80
 - exploiting software
vulnerabilities, 83
 - fraud, 116
 - SIP authentication
dictionary attack, 80-82
 - unified messaging
servers, 337
 - user authentication
 - carrier-grade VoIP
architecture, 329
 - enterprise VoIP, 343
 - SRTP, 224
 - User Datagram Protocol
(UDP), 10
 - User-Authorization-Answer
(UAA) command, 278
 - User-Authorization-Request
(UAR) command, 278
- V**
- verification, 160
 - VLANs (virtual LANS), 342
 - eavesdropping, 93-94
 - voice mail servers, 336
 - Voice over IP. *See* VoIP
 - voicemail, 61
 - VoIP, 1
 - carrier-grade VoIP. *See*
carrier-grade VoIP
architectures
 - closed VoIP, 13
 - deployments, 12-13, 15
 - enterprise VoIP. *See*
enterprise VoIP
 - Internet-based VoIP, 12
 - IP communications
and, 9-12
 - risk analysis, 18-20
 - security, challenges
of, 15-17
 - telecommunications
and, 4-7
 - wireless VoIP, 14
 - VOIP-01 insufficient verifica-
tion of data, 144-146
 - VOIP-02 execution flaws, 146
 - VOIP-03 string/array/
pointer manipulation
flaws, 147-149
 - VOIP-04 low resources, 149
 - VOIP-05 low bandwidth, 150
 - VOIP-06 file/resource
manipulation
flaws, 151-152
 - VOIP-07 password
management, 152
 - VOIP-08 permissions and
privileges, 153
 - VOIP-09 crypto and
randomness, 153-154
 - VOIP-10 authentication
and certificate
errors, 155-157
 - VOIP-11 error
handling, 157-158
 - VOIP-12 homogeneous
network, 158
 - VOIP-13 lacking fallback
system, 158
 - VOIP-14 physical connection
quality and packet
collision, 159

- vulnerabilities, 19
 - analyzing, 160-162
 - attack categories and security requirements, 129-130
 - configuration management, 159-160
 - creation of, 128
- CWE
 - CWE-01 insufficient verification of data, 130-131
 - CWE-02 pointer issues, 131
 - CWE-03 resource management errors, 132
 - CWE-04 race conditions, 132
 - CWE-05 temporary file issues, 133
 - CWE-06 password management, 133
 - CWE-08 cryptographic errors, 134
 - CWE-08 permissions, privileges, and ACLs, 133
 - CWE-09 randomness and predictability, 135
 - CWE-10 authentication errors, 135-136
 - CWE-11 certificate issues, 136
 - CWE-12 error handling, 137-138
- defined, 55
- exploiting software vulnerabilities, 83
- human behavior, 162-163
- OWASP (Open Web Application Security Project), 139
 - OWASP-02 Cross-Site Scripting (XSS) flaws, 140
 - OWASP-03 injection flaws, 140
 - OWASP-04 buffer overflows, 140
 - OWASP-05 denial of service (DoS), 140
 - OWASP-06 broken access control, 141
 - OWASP-07 insecure storage, 141
 - OWASP-08 broken authentication and session management, 141
 - OWASP-09 improper error handling, 142
 - OWASP-10 insecure configuration management, 142
- OWASP-01 unvalidated input parameters, 139
- VoIP categories, 142-143
 - VOIP-01 insufficient verification of data, 144-146
 - VOIP-02 execution flaws, 146
 - VOIP-03 string/array/pointer manipulation flaws, 147-149
 - VOIP-04 low resources, 149
 - VOIP-05 low bandwidth, 150
 - VOIP-06 file/resource manipulation flaws, 151-152
 - VOIP-07 password management, 152
 - VOIP-08 permissions and privileges, 153
 - VOIP-09 crypto and randomness, 153-154
 - VOIP-10 authentication and certificate errors, 155-157
 - VOIP-11 error handling, 157-158
 - VOIP-12 homogeneous network, 158
 - VOIP-13 lacking fallback system, 158
 - VOIP-14 physical connection quality and packet collision, 159
- W-X-Y-Z**
- wireless VoIP, 14
- Wireshark, 85-86
- XSS (Cross-Site Scripting), 140
- Zfone, 256-257
- ZID variable (ZRTP key negotiation), 254
- ZRTP
 - DoS, 258
 - DTMF (Dual Tone Multi Frequency) disclosure, 259-260
 - key negotiation, 251-256
 - man-in-the-middle attacks, 258
 - overview, 251
 - Zfone, 256-257