

# Index

- 3GPP2, *see* Third Generation Partnership Project 2
- 802.11I 236, 238, 260
- 802.1X 43, 55, 237, 238, 259, 260
- AAA
  - AAA application 6, 19
  - AAA Architecture group 10, 19
  - AAA key for Mobile IP signaling 167, 181
  - AAA key in EAP key management framework 52, 56
  - AAA server 6, 7, 20–1, 44, 52, 167, 181, 193
  - AAASA 179
- AA-answer (Diameter NAS) 165
- AA-Mobile node Answer 190
- AA-Mobile node Request 190, 194
- AA-request 164, 165
- Access control 21, 41
- Access control list
  - host-based access control list (PKI for IPsec) 231
  - user-based access control list 231
- Access network discovery 115
- Access point
  - light-weight access point 114
  - new access point 115, 123
  - old access point 115, 123
- Access router
  - candidate access router 115, 118, 119
  - current access router 115
  - target access router 115
- Access technology 7, 56, 118, 266, 272
- Accounting
  - application 13
  - data 15
  - event driven models 15
  - interim 14, 18
  - management 13
  - metrics 14
  - proxy 14
  - records 17
  - reliability 17, 140, 162, 163
  - request 128
  - server 14
  - server fail-over 18
- Administrative domain
  - home administrative domain 10, 167
  - visited administrative domain 10, 113
- AES, *see* American Encryption Standard
- Agent advertisement
  - agent advertisement challenge extension 109, 184
- Agent sequence 12
- American Encryption Standard 50
- Anonymous key exchange 39
- Anti-replay protection 36, 65, 108
- Application
  - application specific information 20, 22
  - application specific module 19, 20
  - diameter application 149, 151, 162
  - identifier (diameter) 151, 158
  - server 11, 65, 236
- Application-specific module 19, 20
- AR, *see* Access router
- ARL (pki4ipsec) 230
- ASM, *see* Application-specific module
- Asymmetric key algorithms 50
- ATIS 268
- Attribute
  - attribute hiding 132
  - attribute value pair (diameter) 154, 155, 156, 165, 190, 253
  - vendor specific 130, 144, 176, 197
- Auditing 13
- Auth-Grace-period (in Diameter NAS) 166
- Authentication
  - device authentication 2, 31
  - message authentication 4, 33

- Authentication (*Continued*)
  - mutual authentication 5, 33, 40
  - port-based authentication 259
  - user authentication 2, 26, 27, 283
- Authentication extension
  - generalized Mobile IP authentication extension 184
  - home-foreign authentication extension 108, 184, 200
  - MN-AAA authentication extension 183, 184, 197
  - mobile-foreign authentication extension 108, 184, 195
  - mobile-home authentication extension 108, 180, 184, 195
- Authentication header 73, 74
- Authentication model
  - three-party authentication model 6, 29, 42, 55, 237, 261
  - two-party authentication model 6, 44, 57, 243, 248
- Authentication server
  - backend authentication server 43, 55, 127, 237
- Authentication token 33, 36
- Authenticator 6, 27, 32, 44, 55, 57, 74, 107, 131, 141, 240, 243, 259
- Authority revocation list (pki4ipsec) 230
- Authorization
  - authorization application 8, 10
  - response 162
- Authorization-lifetime AVP 166
- Authorization-only (in Diameter NAS) 166
- AVP
  - AVP code 156, 164, 253
  - CHAP-algorithm AVP 165
  - CHAP-Auth AVP 165, 172
  - CHAP-challenge AVP 165
  - CHAP-ident AVP 165
  - CHAP-response AVP 172
  - destination host AVP 156, 159
  - destination realm AVP 157, 159
  - MIP-feature-vector AVP 193
  - MIP-MN-AAA-Auth 191, 193
  - NAS authentication AVP 165
  - NAS authorization AVP 165
  - origin host AVP 154, 156, 172
  - origin realm AVP 156
  - password-retry AVP 165
  - result-code AVP 155, 157
  - user-password AVP 165
- Backoff mechanism 141
- Backward compatibility 129, 130, 144, 152, 170, 185
- Berkley Internet Name Domain (DNS) 112, 170, 224
- BET, *see* Bi-directional edge tunnel
- Bi-directional edge tunnel 116
- Bilateral agreements 143, 272, 280
- Billing
  - non usage sensitive billing 17
  - server 13
  - usage sensitive billing 17
- BIND, *see* Berkley Internet Name Domain (DNS)
- Binding update 114
- Bootstrapping, *see* Mobile IP, bootstrapping
- CA, *see* Certificate authority
- Candidate access router 115, 118
- Candidate access router discovery protocol 116, 118, 119
- Capability discovery 118, 119
- Capability exchange 159, 163
- Capability negotiation 143, 151, 159, 169
- Capability pre-filtering 120
- CARD (Candidate access router discovery) 116, 118, 119
  - CARD reply 119
  - CARD request 119, 120
  - preference sub-option 120
  - requirement sub-option 120
- Care of address
  - collocated care of address 102, 189
  - FA CoA 102, 189
- CcOA, *see* Collocated care of address
- CDMA2000 26, 196
- CEP, *see* Certificate enrollment protocol
- CERT 228
- Certificate
  - certificate 228
  - certificate payload 228
  - certificate request 84, 206, 211, 217, 219, 220, 229, 247
  - certificate revocation 206, 210, 211, 225
  - certificate revocation list 210, 230
  - certificate status checking 207
  - certificate type 93, 227
  - device certificate 226, 248
  - subject name 205, 211, 223
  - user certificate 224, 226
  - X.509 certificate 22, 197, 205
- Certificate authority
  - trust anchor certificate authority 207, 230

- Certificate enrollment protocol 213, 221
- Certificate management protocol 219
- Certificate management using CMS 213, 221
- Certificate request message format 214, 219
- Certificate revocation list 210, 230
- Certification 206, 212, 225, 226
- CERTREQ 84, 228
- Challenge 109, 184
  - agent advertisement challenge extension 109, 184
  - Mobile-Foreign challenge extension 109, 184, 193
- Challenge handshake authentication protocol
- CHAP, *see* Challenge handshake authentication protocol
- Chargeable user identity 284
- Cipher suite 56, 58, 93, 252, 256
- Cipher suite independence 58
- Circle of trust 276, 278
- CMC, *see* Certificate management using CMS
- CMP, *see* Certificate management protocol
- CoA, *see* Care of address
- Collocated care of address 102, 189
- Command, *see* Diameter
- Command code, *see* Diameter
- Congestion control 18, 124, 157
- Connection (Diameter) 95, 136, 150, 157, 162
- Context data block 122, 125
- Context transfer
  - context transfer activate request 125
  - context transfer data 125
  - context transfer data reply 125
  - proactive context transfer 124
  - reactive context transfer 125
  - time efficient context transfer 121, 123
- Context transfer protocol 121
- Contractual relationship 10
- Converged networks 268, 274
- Cookie 82, 282
- COPS 147
- Correspondent node 100, 106
- Cost allocation 13
- CRC, *see* Cyclic redundancy checks
- Credit control
  - credit control server 152
- CRL, *see* Certificate revocation list
- CRL server 207, 210
- CRMF, *see* Certificate request message format
- Crypto period
- Cryptographic key
- CTP, *see* Context transfer protocol
- Cyclic redundancy checks 4, 26
- Data encryption standards 68, 75, 85
- Data integrity protection 4, 33, 74
- Denial of service attack 107, 123
- DES, *see* Data encryption standards
- DH, *see* Diffie-Hellman
- Diameter
  - AA-answer 164, 165
  - AA-Mobile node Answer 190
  - AA-Mobile node Request 190
  - AA-request 164
  - accounting 149, 151, 162
  - AMA, *see* AA-Mobile node Answer
  - AMR, *see* AA-Mobile node Request
  - application 149, 151, 156, 159, 162, 167, 188
  - application identifier 151, 158
  - AVP 153, 155, 157, 164, 190, 193, 253
  - backward compatibility 130, 170
  - base protocol 148, 150, 156, 164
  - capability negotiation 143, 151, 159, 169
  - client 149, 152
  - command 171, 190
  - command code 154, 189
  - credit control 151, 155
  - EAP 152, 167
  - EAP answer 167, 168, 245, 256
  - EAP application 163, 167
  - EAP request 42, 167, 237, 244
  - HMA, *see* Home agent MIP-Answer
  - HMR, *see* Home agent MIP-Request
  - Home agent MIP-Answer 190, 195
  - Home agent MIP-Request 190, 194
  - mandatory bit 156
  - MIP-Feature-Vector AVP 193
  - Mobile IP application 152, 165, 167, 188, 190
  - Mobile IP AVPs 188
  - NASREQ application 152, 167
  - node 151, 152
  - peer table 158
  - re-authentication 164, 166
  - re-authorization 164
  - realm based routing table 158
  - server 149, 151, 153, 162, 165, 189
  - session 160
- Diameter Agent
  - proxy agent 153
  - redirect agent 153
  - relay agent 142, 153
  - translation agent 153, 166, 171

- Dictionary attack 29, 37, 235
- Diffie-Hellman
  - content encryption keys 59
  - key encryption keys 48, 60
- Digest 4, 27, 34, 37, 39, 41, 68, 216
- Discovery service 277
- DNS 170, 224
- DOI, *see* Domain of Interpretation
- Domain 14, 208, 226
- Domain name (dns appendix) 172, 223, 224
- Domain name servers 224
- Domain of Interpretation 80
- DoS, *see* Denial of service attack
- Downgrade attacks 41
- EAP
  - EAP authentication method 44, 58, 241
  - EAP authentication phase 26, 44, 56
  - EAP discovery phase 56
  - EAP key management 43, 54, 55, 57, 238
  - EAP key transport phase 56
  - EAP methods 240, 241
  - EAP request 42, 138, 237
  - EAP request identity 43, 237, 246
  - EAP response 42, 138, 238, 246, 255
  - EAP server 44, 55, 57, 168, 242, 246
  - EAP-Message attribute 139
  - EAP-SIM 236, 257
  - EAP-TLS 43, 244, 248
  - EAP-TTLS 40, 248, 250, 252, 254, 255, 262, 284
  - EAP-XXX 242
- EAPOL 237, 260
- E-commerce 5, 40, 92, 249, 281
- Encapsulating security payload 73, 74
- End to end identifier 154
- End-to-end security 156, 160, 168
- Ephemeral key 48
- Extensible authentication protocol, *see* EAP
- FA, *see* Foreign agent
- Failover 168
- Fast Mobile IP 115
- Feature profile type 122
- Federal Information Processing Standards 33
- Federated Network Identity 275, 276
- FIPS, *see* Federal Information Processing Standards
- Flooding attack 60
- FMIP, *see* Fast Mobile IP
- Foreign agent 100, 102, 106, 152, 177, 189
- Forward tunneling 76, 101
- FPT, *see* Feature profile type
- FQDN, *see* FQDN
- Fragmentation 239
- FreeRADIUS 145
- FreeS/WAN 97
- Fully qualified domain name 172, 224
- Generic authentication framework 41, 55
- Group key 48
- GSM
  - GSM triplets 257
- HA, *see* Home agent
- HAAA, *see* Home AAA server
- Handover
  - fast handover 114, 117
  - heterogeneous handover 114
  - homogeneous handover 114
  - layer 2 handover 115
  - layer 3 handover 113, 116, 120
  - low-latency handover 115, 120
  - mobile-controlled handover 114
  - network-controlled handover 114
  - seamless handover 117, 248
  - smooth handover 117
- Hash
  - hash algorithm 4, 29, 34, 37, 50, 107
  - hash function 4, 34, 50, 74, 87
  - keyed hash function 34, 87
  - secure hash algorithm 36, 75
- Header compression 26, 121, 123
- HMAC 34, 75, 107
- HoA, *see* Home address
- Home AAA server 10, 12, 189, 250
- Home address 99, 111
- Home agent
  - dynamic home agent assignment 111
  - local home agent 111
  - redirected HA 113
  - requested HA 112
- Home agent MIP-Answer 190, 195
- Home agent MIP-Request 190, 194
- Hop-by-hop identifier 154
- HTML form 40
- HTTP 38, 221, 281
- HTTP basic authentication 38
- HTTP digest authentication 39
- IAB, *see* Internet architecture board
- IANA 43, 122, 156

- Identity federation 276
  - Identity services 275, 276
  - IESG, *see* Internet Engineering Steering Group
  - IETF
    - AAA working group 10, 19, 147, 150, 162, 172
    - IPsec working group 78, 228
    - Mobile IP working group 118, 176
    - PKIX working group 209, 227
  - IKE
    - aggressive mode 83, 87, 89
    - IKE authentication 80, 86, 88, 197, 230
    - IKE phases 80, 81, 82
    - IKE pre-shared keys 52, 53, 62, 66, 67, 88, 89, 198, 227
    - IKE SA 80, 82, 86
    - main mode 81, 88
    - new group mode 83
    - phase 1 81, 83, 86, 88, 89, 195, 231
    - phase 2 57, 80, 82, 87, 161
    - quick mode 82
  - Information-theory code 4
  - Initialization vector 48
  - Internet architecture board 25
  - Internet Assigned Number Authority, *see* IANA
  - Internet Engineering Steering Group 130
  - Internet Engineering Task Force, *see* IETF
  - Internet Key Exchange, *see* IKE
  - Internet Protocol Security 73
  - Internet Research Task force 10
  - Internet security association and key management protocol, *see* ISAKMP
  - IP in IP encapsulation 100
  - IPsec
    - AH, *see* Authentication header
    - authentication header 74
    - domain of interpretation 80
    - encapsulating security payload 74
    - ESP, *see* Encapsulating security payload
    - inbound processing 79
    - integrity checksum value 74
    - outbound processing 78
    - SA 10, 54, 57, 77, 78, 85, 177, 178
    - security association 10, 54, 57, 77, 78, 85, 177, 178
    - transport mode 76
    - tunnel mode 76
  - IRTF, *see* Internet Research Task Force
  - ISAKMP
    - ISAKMP aggressive exchange 83
    - ISAKMP exchange type 84
    - ISAKMP header 84
    - ISAKMP identity protect exchange 83
    - ISAKMP payload 80, 83, 84, 86, 228
    - ISAKMP phases 80, 81
    - ISAKMP SA 80, 84, 87
    - ISAKMP security association payload 80, 81, 86
  - KDC, *see* Key distribution center
  - Kerberized internet negotiation of keys 66
  - Kerberos
    - Kerberos authentication server 63
    - Kerberos authentication service request 63
  - Key agreement 52, 58, 61
  - Key de-registration 48
  - Key distribution
    - key distribution center 63
    - manual key distribution 53
  - Key distribution center 63
  - Key encryption key 48, 60
  - Key establishment scheme 51
  - Key labeling 48, 52
  - Key management policy 51
  - Key refresh 57, 61, 82
  - Key registration 48
  - Key revocation 48
  - Key transport 51, 56
  - Key type 49, 52
  - Key wrapping 49, 53
  - Keying material 48, 51, 87
  - KINK 66
  - KRB\_AS\_REP 64
  - KRB\_AS\_REQ 63
  - KRB\_TGS\_REP 65
  - KRB\_TGS\_REQ 64
- LAAA, *see* Local AAA server
  - Layer-2
    - device 114
    - function 114
    - handover 115
    - trigger 114 *passim*
  - LCP, *see* Link control protocol
  - LEAP 136, 144, 241, 260
  - Liberty alliance
    - discovery service 277
    - identity provider 276, 278, 279
    - identity service 275, 276
    - permission-based attribute sharing 278
  - Liberty-enabled sites 281
  - Liberty Identity-Federation Framework 275

- Liberty Identity Services Interfaces
  - Specifications 276
- Liberty Identity Web Services Framework 275, 277, 281
- Link control protocol 26
- Linked identities 276
- Local AAA server 12, 177, 189
- Local proxy 14
- Lock-step protocol 239
  
- MAC, *see* Message authentication code
- Man-in-the-middle attack 143, 271
- Manual key transport 49
- Master key 49, 63, 87, 95
- Maximum transmission unit 239
- M-bit 156
- MS-CHAP 144, 249, 260
- MD5 34, 74, 86, 164, 185, 198
- Media access control
  - MAC address 58, 222
- Media independence 58
- Message authentication code 34, 95, 258
- Message Authenticator, *see* RADIUS
- Message authenticator attribute 132, 139, 171
- MITM, *see* Man-in-the-middle attack
- MN, *see* Mobile node
- Mobike 91
- Mobile Foreign challenge extension 109, 184, 193
- Mobile IP
  - agent advertisement 102, 109
  - agent advertisement challenge extension 109, 184
  - agent discovery 102
  - authentication extensions 107, 108, 179, 184, 199
  - binding update 114
  - bootstrapping 110, 113
  - de-tunneling 100
  - dynamic home address assignment 111
  - dynamic home agent assignment 111
  - key generation nonce reply extension 186, 195
  - key generation nonce request extension 186, 193
  - local home agent assignment 111
  - redirected HA extension 113
  - registration life time 100, 103, 105, 107
  - registration reply 103, 107, 113, 183
  - registration request 103, 107, 112, 167, 176, 181 *passim*
  - requested ha extension 112
  - reverse tunneling 103, 106
  - security 101, 103, 106 *passim*
  - tunneling 103
- Mobile IP-AAA signaling 176, 177, 179, 182, 186, 188, 196
- Mobile IPv4 101, 105, 108, 111, 152, 167, 176, 184, 188
- Mobile IPv6 102, 109
- Mobile node 52, 99, 111, 167, 176, 181, 188, 190
- Mobility binding 100
- Mobility security association 179
- MSA, *see* Mobility security association
- MTU, *see* Maximum transmission unit
  
- NAI, *see* Network access identifier
- NAS, *see* Network access server
- NASREQ 151, 160, 163, 164
- NAT, *see* Network address translator
- National Institute of Standards and Technology 47
- NCP, *see* Network control protocol
- Nemo, *see* Network mobility
- Network access identifier 14, 111, 223, 271
- Network access server 6, 21, 127, 152, 163
- Network address translator 91
- Network control protocol 26
- Network discovery 118, 262
- Network interface card 260, 261
- Network mobility 52, 110, 125
- Network selection 118
- Network time protocol 64
- NIC, *see* Network interface card
- NIST, *see* National Institute of Standards and Technology
- Nonce 49, 52, 61, 81, 82, 89–90, 93–4, 108, 179, 181–3, 186, 190, 193–5, 197, 220
  - nonce reply extension 183, 186, 187, 195
  - nonce request extension 183, 186, 193, 195, 197
- Oakley 80, 85, 90
- One-time password 37, 38, 40, 42, 165, 241, 242, 262
- Online certificate status protocol 207, 210, 222
- Open source implementation 97, 145, 172
- OPENSSL 97
- OSCP, *see* Online certificate status protocol
- OTP, *see* One-time password
  
- Packet cable 68
- Packet Data Service Node 196

- Pairwise key 48, 49, 50
- PANA, *see* Protocol for carrying authentication for network access
- PAP, *see* Password authentication protocol
- Password
  - one-time password 37, 38, 40, 42, 165, 241, 242, 262
  - password authentication protocol 26, 135, 235
  - password file 37, 38
  - password sniffing 38, 249
- Password authentication protocol 26, 135, 235
- PDP, *see* Policy decision point
- PDSN, *see* Packet Data Service Node
- PEAP 145, 241, 242, 262, 284
- Peer 43, 152, 158, 170
- Peer-to-peer 52, 54, 66, 79, 81, 91, 163, 171, 243, 244, 245, 269, 281
- Peer-to-peer security 161
- Perfect forward secrecy 49, 62
- PFS, *see* Perfect forward secrecy
- PKCS#10 213, 214–15, 216, 218, 219
- PKCS#7 213, 214, 216, 218, 230
- PKI
  - PKI management functions 178, 210, 219, 249
  - PKI management protocols 210, 212, 213, 214, 219, 221, 222
  - registration 206
- PKI4IPsec 91, 228, 232
- PKINIT 66
- Point of presence 21, 30, 71, 114, 259
- Point-to-point protocol 8, 26, 135, 244
- Policy 12
  - policy decision point 12
  - policy framework 12, 13, 23
  - policy repository 12, 20, 21
  - policy server 12, 13
- Policy decision point 12
- Polling model 15–16
- POP, *see* Point of presence
- PPP, *see* Point-to-point protocol
  - PPP extension working group 30, 45, 262
  - PPP frame 26 *passim*, 237
- Pre-paid (Diameter) 8, 9, 19, 151
- Private key 32–3, 40–1, 50, 52, 57, 59, 60, 67, 68
  - password based private key 32–3, 40–1
- Proof of possession 206, 211–12, 219
- Protocol for carrying authentication for network access 45
- Proxy
  - diameter proxy 149, 150, 168
  - RADIUS proxy 134, 142
- Proxy chaining 134, 142, 143, 170
- Public key 32, 52, 67
- Public key algorithms 50
- Public key certificate 47, 50, 60, 61, 66, 68, 80, 203, 204
- Public key cryptography for initial authentication in kerberos 66
- Public key infrastructure, *see* PKI
- Public seed 49
- Pull sequence 12
- Push sequence 12
- Quality of service, QoS 8, 19, 64, 91, 271
- RADIUS 7, 15, 19, 22, 127 *passim*, 176 *passim*, 237, 239, 249 *passim*
  - access accept 128, 132, 136, 137, 183, 198–200
  - access challenge 127, 129, 130, 131, 137
  - access reject 128, 130, 132, 136, 137
  - access request 127 *passim*, 198–200
  - accounting 139
  - accounting request 128, 132, 139, 141
  - accounting response 128, 139, 141
  - attributes 129, 130, 132, 134, 136, 143, 144
  - client 127 *passim*
  - EAP-Message attribute 139
  - message-authenticator attribute 132, 139, 171
  - request authenticator 131, 132, 133, 136, 137, 141
  - response authenticator 131, 132, 141
  - vendor-specific attributes 130, 144, 176, 197
  - VSA, *see* Vendor-specific attributes
- RADIUS++ 147, 148
- Re-auth-answer (Diameter) 155, 164
- Re-auth-request (Diameter) 155, 164
- Re-keying 49, 82, 123
- Reassembly 239
- Registration reply 103 *passim*, 183, 186, 190, 193, 195, 200
- Registration request 103, 104, 105, 107–9, 111–13, 167, 176 *passim*
- Relay agent 142, 153, 156
- Replay attack 36, 37, 38, 49, 60, 81, 108, 131
- Resource management
  - layer-2 resource management 114
- Result-Code AVP (Diameter NAS) 155, 157, 160, 164 *passim*, 181, 190
- Retransmission 43, 61, 123, 131, 141, 169, 239

- Retransmission behavior 18
- Reverse address translation 115, 116, 119
- Reverse tunneling 103, 106
  - direct delivery style 106
  - encapsulated delivery style 106
- Roaming agreements 15, 118, 142, 269
- Roaming operations 141, 158, 284
- Roaming relationship path 142, 143
- ROAMOPS 141, 142
- Robust secure network 58
- RSN, *see* Robust secure network
  
- SA, *see* Security association
- SADB, *see* Security association database
- Salt, salting 37, 38, 49, 134
- SCEP, *see* Simple certificate enrollment protocol
- SCTP 18, 123, 124, 148, 150, 157, 158, 169, 170, 239, 245
- SDO, *see* Standard Development Organization
- Seamless mobility 110, 116, 117, 118, 121
- Seamoby 116, 118, 121
- Secret seed 49
- Secure association protocol 58
- Secure hash standard 34–6, 75
- Secure shell 39
- Secure socket layer 39, 92, 213, 215
- SecureID card 37, 38
- Security association 10, 54, 57, 77, 78, 80, 81, 85, 117, 123, 161, 175, 178, 179, 180, 197
  - AAA security association 54, 57, 161, 175 *passim*, 180, 251, 254
  - mobility security association 179, 180
  - pre-established security associations 251
  - security association database 78
- Security association database 78
- Security gateway 72, 73, 76, 77
- Security parameter index 77, 108, 179, 180
- Security policy database 78, 110
- Server-initiated messages 156, 169, 171
- SHA1, *see* Secure hash standard
- SIM, *see* Subscriber identity module
  - SIM-based authentication 30, 31, 224, 257, 258
- Simple certificate enrollment protocol 213, 221
- Single sign-on 62, 63, 275, 276, 279, 281, 282, 283
- Single sign out 281
- SKEME 80, 90
- Sniffing attack 37, 38
- SNMP 114, 147, 148
- SOAP 281
- SPD, *see* Security policy database
  - SPD selector 78, 79
- SPI, *see* Security parameter index
- Spoofing attack 60, 74
- SSH, *see* Secure shell
- SSL, *see* Secure socket layer
- Standard Development Organization 196
- Stream Control Transport Protocol, *see* SCTP
- Subscriber identity module 30, 257
- Supplicant 6, 8, 26, 43, 128, 237, 244, 260
- Symmetric key algorithms 50, 75
  
- Tamper-evident 32, 40, 225
- Tamper-proof 205, 214, 225
- Target access router 120
- TCP (Diameter) 148, 150, 157, 158, 169, 170, 239
- Third Generation Partnership Project 2 196
- Threat model
  - threat model analysis 44
- Ticket granting server 63
- Ticket granting ticket 63
- TLS
  - alert protocol 95
  - certificate verify 93
  - client certificate 94
  - client hello 93
  - client key exchange 93
  - finished 93
  - master secret 94
  - pre-master secret 94
  - server hello 93
  - TLS handshake protocol 92, 95
  - TLS record protocol 92, 95
- Token 33, 36, 41, 125
- Transient EAP key 56
- Transient session key 57
- Translation agent 153, 163, 171
- Transport layer protocol 22
- Transport layer security 44, 60, 73, 91, 96, 149
- Trend analysis 13, 18
- Triggers
  - layer-2 trigger 114
- Trust model 177
- Trust relationship 10, 40
- TTLS
  - TTLS challenge 256
  - TTLS server 250, 253, 254, 256
- Tunneled TLS, *see* TTLS
- Tunneling 100, 103 *passim*
  
- Vendor-specific attributes 130, 197, 198
- VPN
  - VPN gateway 72, 91, 210, 231, 251, 266

- W3C, *see* World Wide Web consortium
- Web redirect 281, 286
- WEP, *see* Wired equivalent privacy
- Wi-Fi alliance 54
- Windows NT key 261
- Wired equivalent privacy 53, 260
- Wireless Local Area Networks (WLAN) 29, 54
- Wireless transport layer security 55
- WLAN 802.11 119, 175
- World Wide Web consortium 279, 281
- WTLS 96
- X.509 certificate 22, 197, 205, 207, 217, 228, 230, 279





