

---

# Table des matières

---

<b>Avant-propos</b> . . . . .	11
<b>Chapitre 1. Introduction à la cryptographie.</b> . . . . .	29
1.1. La fonction de chiffrement. . . . .	29
1.1.1. L'algorithme 3DES. . . . .	30
1.1.2. L'algorithme AES . . . . .	34
1.1.3. L'algorithme RSA . . . . .	37
1.1.4. L'algorithme ECC . . . . .	38
1.2. La fonction de hachage . . . . .	39
1.2.1. L'algorithme MD5 . . . . .	39
1.2.2. L'algorithme SHA . . . . .	42
1.2.2.1. L'algorithme SHA-1 . . . . .	42
1.2.2.2. L'algorithme SHA-2 . . . . .	43
1.2.3. Le mécanisme HMAC . . . . .	45
1.3. L'échange de clés . . . . .	47
1.3.1. La génération de la clé secrète . . . . .	47
1.3.2. La distribution de la clé publique. . . . .	48
<b>Chapitre 2. Le mécanisme 802.1x</b> . . . . .	51
2.1. Présentation générale . . . . .	51
2.2. Le protocole EAPOL . . . . .	52
2.2.1. Le message EAPOL- <i>Start</i> . . . . .	53
2.2.2. Le message EAPOL- <i>Logoff</i> . . . . .	53
2.2.3. Le message EAPOL- <i>Key</i> . . . . .	53
2.2.4. Le message EAPOL- <i>Encapsulated-ASF-Alert</i> . . . . .	54
2.2.5. Le message EAPOL-MKA . . . . .	54

---

2.2.6. Le message EAPOL- <i>Announcement</i> . . . . .	54
2.2.7. Le message EAPOL- <i>Announcement-Req</i> . . . . .	54
2.3. Le protocole EAP . . . . .	55
2.3.1. EAP- <i>Method Identity</i> . . . . .	57
2.3.2. EAP- <i>Method Notification</i> . . . . .	58
2.3.3. EAP- <i>Method NAK</i> . . . . .	58
2.4. Le protocole RADIUS . . . . .	58
2.4.1. Les messages RADIUS . . . . .	60
2.4.1.1. Le message <i>Access-Request</i> . . . . .	60
2.4.1.2. Le message <i>Access-Challenge</i> . . . . .	60
2.4.1.3. Le message <i>Access-Accept</i> . . . . .	60
2.4.1.4. Le message <i>Access-Reject</i> . . . . .	60
2.4.2. Les attributs RADIUS . . . . .	60
2.4.2.1. L'attribut EAP- <i>Message</i> . . . . .	61
2.4.2.2. L'attribut <i>Message-Authenticator</i> . . . . .	61
2.4.2.3. L'attribut <i>Password-Retry</i> . . . . .	61
2.4.2.4. L'attribut <i>User-Name</i> . . . . .	61
2.4.2.5. L'attribut <i>User-Password</i> . . . . .	61
2.4.2.6. L'attribut <i>NAS-IP-Address</i> . . . . .	62
2.4.2.7. L'attribut <i>NAS-Port</i> . . . . .	62
2.4.2.8. L'attribut <i>Service-Type</i> . . . . .	62
2.4.2.9. L'attribut <i>Vendor-Specific</i> . . . . .	62
2.4.2.10. L'attribut <i>Session-Timeout</i> . . . . .	62
2.4.2.11. L'attribut <i>Idle-Timeout</i> . . . . .	62
2.4.2.12. L'attribut <i>Termination-Action</i> . . . . .	63
2.5. Les procédures d'authentification. . . . .	63
2.5.1. La procédure EAP-MD5 . . . . .	64
2.5.2. La procédure EAP-TLS . . . . .	65
2.5.3. La procédure EAP-TTLS . . . . .	67
<b>Chapitre 3. Les mécanismes WPA.</b> . . . . .	<b>69</b>
3.1. Introduction à la technologie Wi-Fi . . . . .	69
3.2. Les mécanismes de sécurité . . . . .	71
3.3. Les politiques de sécurité. . . . .	72
3.4. La gestion des clés. . . . .	75
3.4.1. La hiérarchie des clés. . . . .	75
3.4.2. Les messages EAPOL- <i>Key</i> . . . . .	76
3.4.3. La procédure <i>4-Way Handshake</i> . . . . .	78
3.4.4. La procédure <i>Group Key Handshake</i> . . . . .	81
3.5. Le protocole WEP . . . . .	82

---

3.6. Le protocole TKIP . . . . .	84
3.7. Le protocole CCMP . . . . .	87
<b>Chapitre 4. Le mécanisme IPSec . . . . .</b>	<b>89</b>
4.1. Rappel sur les protocoles IP . . . . .	89
4.1.1. Le protocole IPv4 . . . . .	89
4.1.2. Le protocole IPv6 . . . . .	92
4.2. L'architecture IPSec . . . . .	94
4.2.1. Les en-têtes de sécurité. . . . .	95
4.2.1.1. L'extension AH. . . . .	95
4.2.1.2. L'extension ESP . . . . .	96
4.2.1.3. Les modes . . . . .	97
4.2.2. L'association de sécurité. . . . .	99
4.2.3. Le traitement du PMTU . . . . .	101
4.3. Le protocole IKEv2 . . . . .	101
4.3.1. L'en-tête du message. . . . .	102
4.3.2. Les blocs . . . . .	104
4.3.2.1. Le bloc SA. . . . .	104
4.3.2.2. Le bloc KE . . . . .	106
4.3.2.3. Les blocs IDi et IDr . . . . .	106
4.3.2.4. Le bloc CERT. . . . .	107
4.3.2.5. Le bloc CERTREQ. . . . .	107
4.3.2.6. Le bloc AUTH . . . . .	107
4.3.2.7. Les blocs Ni et Nr . . . . .	107
4.3.2.8. Le bloc N . . . . .	108
4.3.2.9. Le bloc D . . . . .	109
4.3.2.10. Le bloc V. . . . .	109
4.3.2.11. Le bloc TS . . . . .	109
4.3.2.12. Le bloc SK . . . . .	109
4.3.2.13. Le bloc CP . . . . .	109
4.3.2.14. Le bloc EAP . . . . .	110
4.3.3. La procédure . . . . .	110
4.3.3.1. L'échange IKE_SA_INIT. . . . .	110
4.3.3.2. L'échange IKE_AUTH . . . . .	112
4.3.3.3. L'échange CREATE_CHILD_SA. . . . .	112
<b>Chapitre 5. Les protocoles SSL / TLS / DTLS . . . . .</b>	<b>115</b>
5.1. Introduction. . . . .	115
5.2. Les protocoles SSL / TLS . . . . .	116

---

5.2.1. L'en-tête <i>Record</i> . . . . .	116
5.2.2. Le message <i>change_cipher_spec</i> . . . . .	117
5.2.3. Le message <i>alert</i> . . . . .	118
5.2.4. Les messages <i>handshake</i> . . . . .	120
5.2.4.1. Le message <i>hello_request</i> . . . . .	121
5.2.4.2. Le message <i>client_hello</i> . . . . .	121
5.2.4.3. Le message <i>hello_server</i> . . . . .	123
5.2.4.4. Le message <i>certificate</i> . . . . .	123
5.2.4.5. Le message <i>server_key_exchange</i> . . . . .	124
5.2.4.6. Le message <i>certificate_request</i> . . . . .	125
5.2.4.7. Le message <i>server_hello_done</i> . . . . .	126
5.2.4.8. Le message <i>client_key_exchange</i> . . . . .	126
5.2.4.9. Le message <i>certificate_verify</i> . . . . .	127
5.2.4.10. Le message <i>finished</i> . . . . .	127
5.2.5. Les informations cryptographiques . . . . .	127
5.2.5.1. La génération des clés . . . . .	127
5.2.5.2. Le contrôle d'intégrité . . . . .	129
5.3. Le protocole DTLS . . . . .	130
5.3.1. L'adaptation au transport UDP . . . . .	130
5.3.1.1. L'en-tête <i>Record</i> . . . . .	130
5.3.1.2. Les messages <i>handshake</i> . . . . .	130
5.3.2. L'adaptation au transport DCCP . . . . .	132
5.3.3. L'adaptation au transport SCTP . . . . .	132
5.3.4. L'adaptation au transport SRTP . . . . .	133
<b>Chapitre 6. La gestion du réseau</b> . . . . .	<b>135</b>
6.1. La gestion SNMPv3 . . . . .	135
6.1.1. Introduction . . . . .	135
6.1.2. L'architecture SNMPv3 . . . . .	136
6.1.2.1. Les applications SNMPv3 . . . . .	137
6.1.2.2. Le moteur SNMPv3 . . . . .	138
6.1.2.3. Le déroulement des opérations . . . . .	141
6.1.3. La structure du message SNMPv3 . . . . .	143
6.2. Le protocole SSH . . . . .	146
6.2.1. Le protocole SSH-TRANS . . . . .	146
6.2.2. Le protocole SSH-USERAUTH . . . . .	149
6.2.3. Le protocole SSH-CONNECT . . . . .	150

<b>Chapitre 7. La technologie MPLS</b> . . . . .	153
7.1. Le réseau MPLS . . . . .	153
7.1.1. L'architecture du réseau . . . . .	153
7.1.2. Les tables du routeur LSR . . . . .	155
7.1.3. La fonction PHP . . . . .	156
7.1.4. Le format de l'en-tête MPLS . . . . .	157
7.1.5. Le support de Diffserv . . . . .	157
7.2. Le protocole LDP . . . . .	159
7.2.1. Les principes de fonctionnement . . . . .	159
7.2.2. Le format du PDU LDP . . . . .	161
7.2.3. Les messages LDP . . . . .	163
7.3. La construction du VPN . . . . .	166
7.3.1. L'architecture du réseau . . . . .	166
7.3.2. La distinction des routes . . . . .	169
7.3.3. La cible de routes . . . . .	170
7.3.4. Les principes de fonctionnement . . . . .	171
7.3.4.1. Le fonctionnement du plan de contrôle . . . . .	171
7.3.4.2. Le fonctionnement du plan de trafic . . . . .	173
7.5. L'interconnexion des réseaux . . . . .	174
7.5.1. Le mode hiérarchique . . . . .	174
7.5.2. Le mode récursif . . . . .	175
<b>Chapitre 8. Le VPN Ethernet</b> . . . . .	177
8.1. La technologie Ethernet . . . . .	177
8.1.1. La couche physique . . . . .	177
8.1.2. La couche MAC . . . . .	179
8.1.3. Le cloisonnement VLAN . . . . .	182
8.2. La technologie PBT . . . . .	184
8.3. La technologie VPLS . . . . .	186
8.3.1. L'architecture du réseau . . . . .	186
8.3.2. L'en-tête EoMPLS . . . . .	189
8.3.3. Le protocole LDP . . . . .	190
8.3.3.1. Le paramètre FEC . . . . .	190
8.3.3.2. Le paramètre <i>PW Status</i> . . . . .	191
8.4. La technologie L2TPv3 . . . . .	191
8.4.1. Le message de données . . . . .	192
8.4.2. Les messages de contrôle . . . . .	193
8.4.3. Les procédures . . . . .	195
8.4.3.1. La gestion de la connexion . . . . .	195
8.4.3.2. La gestion de la session . . . . .	197

<b>Chapitre 9. Les pare-feux</b> . . . . .	201
9.1. Les technologies . . . . .	201
9.1.1. Le filtre de paquets . . . . .	201
9.1.2. La passerelle applicative . . . . .	204
9.1.3. Le dispositif NAT / NAPT . . . . .	204
9.2. La traversée du dispositif NAT / NAPT . . . . .	207
9.2.1. Le protocole ICMP . . . . .	208
9.2.2. Le mécanisme IPSec . . . . .	209
9.2.3. Les protocoles SIP, SDP et RTP . . . . .	210
9.2.3.1. Le protocole STUN . . . . .	212
9.2.3.2. Le protocole TURN . . . . .	212
9.2.3.3. Le mécanisme ICE . . . . .	214
9.2.4. Le protocole FTP . . . . .	215
9.2.5. La fragmentation . . . . .	217
<b>Chapitre 10. La détection d'intrusion</b> . . . . .	219
10.1. La typologie des attaques . . . . .	219
10.2. Les méthodes de détection . . . . .	221
10.2.1. La détection basée sur la signature . . . . .	221
10.2.2. La détection basée sur les anomalies . . . . .	222
10.2.3. L'analyse des protocoles . . . . .	222
10.3. Les technologies . . . . .	223
10.3.1. Le dispositif N-IDPS . . . . .	224
10.3.2. Le dispositif WIDPS . . . . .	226
10.3.3. Le dispositif H-IDPS . . . . .	228
10.3.4. Le dispositif NBA . . . . .	229
<b>Bibliographie</b> . . . . .	231
<b>Liste des abréviations</b> . . . . .	235
<b>Index</b> . . . . .	243