
Contents

PREFACE	xi
ABBREVIATIONS	xxxiii
CHAPTER 1. INTRODUCTION TO CRYPTOGRAPHY	1
1.1. The encryption function	1
1.1.1. 3DES algorithm	3
1.1.2. AES algorithm	6
1.1.3. RSA algorithm	10
1.1.4. ECC algorithm	12
1.2. Hash function	13
1.2.1. MD5 algorithm	13
1.2.2. SHA algorithm	16
1.2.3. HMAC mechanism.	20
1.3. Key exchange.	22
1.3.1. Secret-key generation.	22
1.3.2. Public key distribution	24
CHAPTER 2. 802.1X MECHANISM	27
2.1. General introduction	27
2.2. EAPOL protocol	28
2.2.1. EAPOL-Start message	30
2.2.2. EAPOL-Logoff message	30
2.2.3. EAPOL-Key message	30

2.2.4. EAPOL-Encapsulated-ASF-Alert message	31
2.2.5. EAPOL-MKA message	31
2.2.6. EAPOL-Announcement message	31
2.2.7. EAPOL-Announcement-Req message	32
2.3. EAP protocol	32
2.3.1. EAP-Method Identity	35
2.3.2. EAP-Method Notification	35
2.3.3. EAP-Method NAK	36
2.4. RADIUS protocol	36
2.4.1. RADIUS messages	38
2.4.2. RADIUS attributes	39
2.5. Authentication procedures	42
2.5.1. EAP-MD5 procedure	44
2.5.2. EAP-TLS procedure	45
2.5.3. EAP-TTLS procedure	48
CHAPTER 3. WPA MECHANISMS	51
3.1. Introduction to Wi-Fi technology	51
3.2. Security mechanisms	54
3.3. Security policies	55
3.4. Key management	59
3.4.1. Key hierarchy	59
3.4.2. EAPOL-key messages	61
3.4.3. Four-way handshake procedure	63
3.4.4. Group key handshake procedure	67
3.5. WEP protocol	68
3.6. TKIP protocol	70
3.7. CCMP protocol	73
CHAPTER 4. IPSEC MECHANISM	77
4.1. Review of IP protocols	77
4.1.1. IPv4 protocol	77
4.1.2. IPv6 protocol	80
4.2. IPSec architecture	83
4.2.1. Security headers	85
4.2.2. Security association	89
4.2.3. PMTU processing	92

4.3. IKEv2 protocol	93
4.3.1. Message header	93
4.3.2. Blocks	96
4.3.3. Procedure	102
CHAPTER 5. SSL, TLS AND DTLS PROTOCOLS	109
5.1. Introduction	109
5.2. SSL/TLS protocols	111
5.2.1. Record header	111
5.2.2. Change_cipher_spec message	112
5.2.3. Alert message	112
5.2.4. Handshake messages	114
5.2.5. Cryptographic information	124
5.3. DTLS protocol	126
5.3.1. Adaptation to UDP transport	126
5.3.2. Adaptation to DCCP transport	129
5.3.3. Adaptation to SCTP transport	130
5.3.4. Adaptation to SRTP transport	131
CHAPTER 6. NETWORK MANAGEMENT	133
6.1. SNMPv3 management	133
6.1.1. Introduction	133
6.1.2. SNMPv3 architecture	135
6.1.3. SNMPv3 message structure	143
6.2. SSH protocol	146
6.2.1. SSH-TRANS protocol	146
6.2.2. SSH-USERAUTH protocol	151
6.2.3. SSH-CONNECT protocol	152
CHAPTER 7. MPLS TECHNOLOGY	155
7.1. MPLS overview	155
7.1.1. Network architecture	155
7.1.2. LSR router tables	157
7.1.3. PHP function	158
7.1.4. MPLS header format	159
7.1.5. DiffServ support	160
7.2. LDP protocol	162
7.2.1. Principles of functioning	162

7.2.2. LDP PDU format	165
7.2.3. LDP messages	167
7.3. VPN construction	170
7.3.1. Network architecture	170
7.3.2. Differentiation of routes	174
7.3.3. Route target	175
7.3.4. Principles of operation	177
7.4. Network interconnection	180
7.4.1. Hierarchical mode	181
7.4.2. Recursive mode	182
CHAPTER 8. ETHERNET VPN	185
8.1. Ethernet technology	185
8.1.1. Physical layer	186
8.1.2. MAC layer	188
8.1.3. VLAN isolation	191
8.2. PBT technology	194
8.3. VPLS technology	196
8.3.1. Network architecture	196
8.3.2. EoMPLS header	199
8.3.3. LDP	201
8.4. L2TPv3 technology	203
8.4.1. Data message	203
8.4.2. Control messages	205
8.4.3. Procedures	208
CHAPTER 9. FIREWALLS	215
9.1. Technologies	215
9.1.1. Packet filter	216
9.1.2. Applicative gateway	218
9.1.3. NAT/NAPT device	219
9.2. NAT/NAPT device crossing	222
9.2.1. ICMP protocol	223
9.2.2. IPSec mechanism	224
9.2.3. SIP, SDP and RTP protocols	227
9.2.4. FTP protocol	233
9.2.5. Fragmentation	235

CHAPTER 10. INTRUSION DETECTION	237
10.1. Typology of attacks	237
10.2. Methods of detection	239
10.2.1. Signature-based detection	240
10.2.2. Anomaly-based detection.	240
10.2.3. Protocol analysis	241
10.3. Technologies	242
10.3.1. N-IDPS device.	243
10.3.2. WIDPS device	246
10.3.3. H-IDPS device.	248
10.3.4. NBA device.	249
BIBLIOGRAPHY	253
INDEX.	259