

Table des matières

Avant-propos	XI
1 Courrier électronique	1
1.1 Courrier électronique forgé	1
1.2 Courrier électronique indésirable	4
1.2.1 Introduction au spam	4
1.2.2 Techniques de diffusion du spam	5
1.2.3 Lutte contre le spam	8
1.3 Modèle économique du spam	11
1.4 Lectures complémentaires	12
Exercices	13
Solutions	16
2 Virus et antivirus	23
2.1 Description et classification	23
2.1.1 Virus	25
2.1.2 Vers	27
2.1.3 Chevaux de Troie	29
2.1.4 <i>Backdoors</i>	30
2.1.5 <i>Spywares</i> et <i>adwares</i>	30
2.1.6 <i>Rootkits</i>	30
2.1.7 <i>Canulars</i>	31
2.2 Protection	32
2.2.1 Logiciels antivirus	32

2.2.2	Architecture	34
2.3	Lectures complémentaires	36
	Exercices	37
	Solutions	42
3	Vulnérabilités des applications et des réseaux	49
3.1	Les bases de TCP/IP	49
3.2	Dénis de service	53
3.2.1	SYN flooding	54
3.2.2	Attaques par réflexion (<i>Smurf</i>)	54
3.2.3	Dénis de service distribués	56
3.3	<i>IP Spoofing</i>	58
3.3.1	Le cas de TCP	58
3.3.2	<i>Spoofing</i> de paquets UDP	60
3.4	<i>Sniffing</i>	60
3.5	Vol de session	62
3.5.1	Vol d'une connexion TCP	62
3.5.2	Session HTTP	63
3.6	<i>Exploits</i>	63
3.6.1	Vulnérabilités conceptuelles	63
3.6.2	Failles techniques	64
3.6.3	Failles des applications en ligne	67
3.7	Lectures complémentaires	70
	Exercices	71
	Solutions	83
4	Pare-feux : translation, filtrage et <i>proxies</i>	95
4.1	Pare-feux	95
4.1.1	Principes de base	95
4.1.2	Types de pare-feux	97
4.1.3	Filtrage	98
4.1.4	Translation d'adresses réseau	99
4.1.5	Autres buts	103

4.1.6	Architectures de pare-feux	104
4.1.7	Règles de filtrage	107
4.1.8	Détection d'intrusion	113
4.2	<i>Proxies</i>	116
4.2.1	<i>Proxies</i> HTTP	116
4.2.2	<i>Proxies</i> FTP	119
4.2.3	<i>Proxies</i> SMTP	120
4.2.4	<i>Proxies</i> DNS	121
4.2.5	<i>Proxies</i> SOCKS	121
4.2.6	<i>Proxies</i> HTTPS	122
4.2.7	<i>Proxies</i> inverses	123
4.3	Lectures complémentaires	124
	Exercices	125
	Solutions	141
5	Notions de base en cryptographie	157
5.1	Buts principaux de la cryptographie	158
5.1.1	Confidentialité	158
5.1.2	Authenticité	158
5.1.3	Intégrité	158
5.2	Cryptographie à clef symétrique	159
5.2.1	Algorithmes de chiffrement par bloc et modes de chiffrement	159
5.2.2	Fonctions de hachage	160
5.2.3	MAC	161
5.3	Cryptographie asymétrique	161
5.3.1	Cryptographie symétrique et asymétrique	161
5.3.2	RSA	162
5.3.3	Certificats numériques	163
5.4	Cryptanalyse	164
5.4.1	Recherche exhaustive	164
5.4.2	Attaque des anniversaires	165
5.4.3	Attaques dédiées	165
5.4.4	Attaques par canaux auxiliaires	165

5.4.5	Preuves de sécurité	165
5.5	Lectures complémentaires	166
	Exercices	167
	Solutions	172
6	Communications sécurisées	179
6.1	Réseaux privés virtuels	179
6.1.1	PPTP	180
6.1.2	L2TP	182
6.1.3	IPSec	183
6.2	Sécurité au niveau de la couche transport	188
6.2.1	Protocoles constituant TLS	188
6.2.2	Authentification	189
6.2.3	Implémentation	190
6.3	SSH	190
6.4	Lectures complémentaires	191
	Exercices	193
	Solutions	200
7	Applications sécurisées	209
7.1	Authentification par mot de passe	209
7.1.1	Authentification Unix	210
7.1.2	Authentification Windows	213
7.1.3	Comment les pirates cassent les mots de passe	214
7.1.4	Comment choisir un bon mot de passe	216
7.2	Protocoles de type question/réponse	217
7.3	Kerberos : un protocole d'authentification réseau	219
7.3.1	Description générale	219
7.3.2	Glossaire	220
7.3.3	Contenu des échanges	220
7.4	PGP : <i>Pretty Good Privacy</i>	222
7.4.1	Chiffrement hybride	223
7.4.2	Algorithmes cryptographiques	223

7.4.3	Longueur des clefs	224
7.4.4	Protection des clefs privées	224
7.4.5	Distribution des clefs publiques	224
7.4.6	Révocation des clefs	226
7.4.7	Graphe de confiance	226
7.5	Lectures complémentaires	227
	Exercices	229
	Solutions	243
8	Gestion de la sécurité	261
8.1	Analyse de risque	261
8.2	Documents clefs	262
8.3	Normes ISO 270XX : sécurité des systèmes d'information	263
8.3.1	ISO 27001 : système de management de la sécurité de l'information (SMSI)	264
8.3.2	ISO 27002 : code de bonnes pratiques pour la gestion de la sécurité de l'information	265
8.4	Catalogues de sécurité allemands	266
8.5	Critères communs	267
8.6	Lectures complémentaires	269
	Exercices	270
	Solutions	273
	Sigles et acronymes	277
	Bibliographie	279
	Index	283