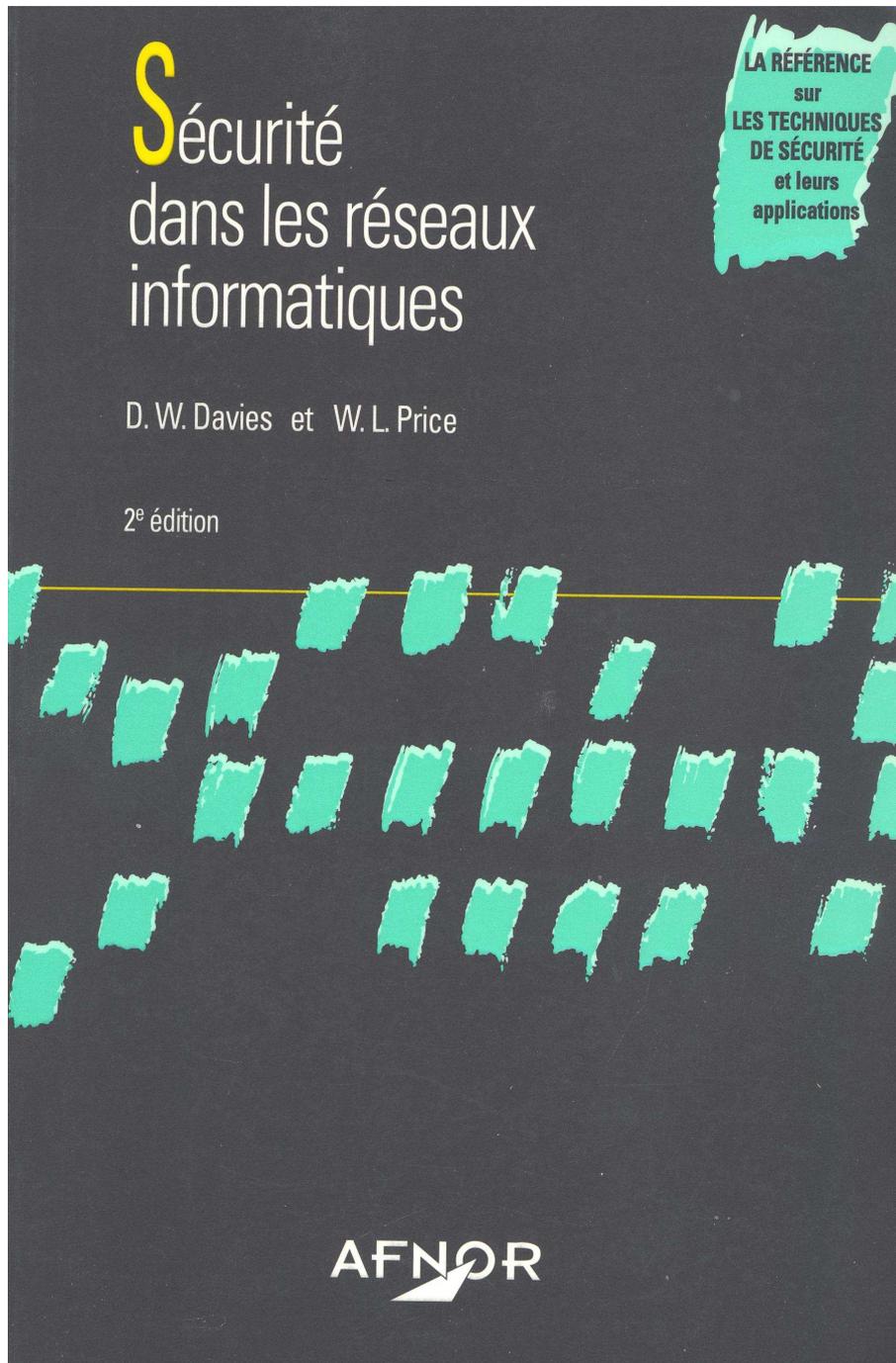




Sécurité dans les réseaux informatiques

Copyright 1995 – 415 pages



Sécurité dans les réseaux informatiques

Restée longtemps l'apanage des activités bancaires et militaires, la sécurité des données concerne maintenant tous les secteurs de l'industrie. En effet, l'information est un facteur essentiel dans la prise de décision et, à ce titre, doit être protégée avec le plus grand soin.

Destiné plus particulièrement au professionnel, qu'il soit dans l'entreprise ou prestataire de services, **Sécurité dans les réseaux informatiques** propose une étude approfondie des schémas de sécurité. Les algorithmes cryptographiques (chiffres), le DES (*Data Encryption Standard*) ou les mécanismes de base tels que l'authentification, l'intégrité, la gestion des clés et les signatures numériques y sont largement décrits. En plus des modifications et mises à jour qui s'imposaient, cette deuxième édition comporte des ajouts sur l'architecture de sécurité du modèle OSI (*Open Systems Interconnection*), la gestion des clés dans le domaine bancaire (qui est également d'un grand intérêt pour les milieux non bancaires) et la description de certains schémas utilisés dans le transfert électronique de fonds.

Illustrant les principes grâce à de nombreux exemples, l'ouvrage **privilégie l'approche pragmatique tout en étant le reflet des derniers développements** en matière de sécurité des données.

«L'idée que la cryptographie constitue l'outil de base de la sécurité des données fait peu à peu son chemin. Ce livre montre comment utiliser la cryptographie pour protéger les données dans les systèmes...»

D. W. Davies et W. L. Price, *Avant-propos à la première édition.*



ISBN 2-12-486517-X

Sommaire

Avant-propos à la première édition	XVII
Avant-propos à la deuxième édition	XXI
Chapitre 1 La sécurité des données	1
1.1 Le besoin de sécurité des données	1
1.2 L'évaluation de la sécurité	4
1.2.1 L'intégrité des logiciels	6
1.2.2 La sécurité et les personnes	8
1.3 L'évolution des technologies et ses conséquences	8
1.4 Les notations pour le chiffrement	10
1.5 Quelques utilisations du chiffrement	13
1.6 Les propriétés générales des fonctions de chiffrement	14
Chapitre 2 Les chiffres et leurs propriétés	17
2.1 Introduction	17
2.2 Les chiffres de substitution	20
2.2.1 Le chiffre de César	20
2.2.2 Les substitutions monoalphabétiques	22
2.2.3 Les substitutions polyalphabétiques	24
2.2.4 Le chiffre de Vigenère	25
2.3 Les chiffres de transposition	28
2.3.1 La transposition simple	28
2.3.2 Le chiffre nihiliste	29

VIII *Table des matières*

2.4	Les chiffres composés	30
2.5	Les machines à chiffrer	31
2.5.1	Le cylindre de Jefferson	31
2.5.2	Le disque de Wheatstone	32
2.5.3	Les machines à rotor: Enigma	33
2.5.4	Les machines à écrire et à chiffrer	35
2.5.5	Les machines à chiffrer modernes	36
2.5.6	Les substitutions dans les chiffres modernes	36
2.5.7	Les substitutions dépendant d'une clé	37
2.5.8	Les transpositions dans les chiffres modernes	37
2.6	Les attaques contre les données chiffrées	38
2.7	Le chiffrement en série	40
2.7.1	Le chiffre de Vernam	41
2.7.2	La suite chiffrante pseudo-aléatoire	42
2.8	Le chiffrement par blocs	43
2.9	La mesure de la solidité d'un chiffre	44
2.9.1	La théorie de Shannon sur les systèmes secrets	44
2.9.2	Les limites de calcul	45
2.9.3	Une application de la théorie de Shannon	46
2.10	Les menaces contre un système sécurisé	46
2.10.1	Les branchements actifs	47
2.10.2	Les méthodes de protection	49
2.11	Les clés de chiffrement	49
	Chapitre 3 La norme <i>Data Encryption Standard</i> (DES)	51
3.1	L'historique du DES	51
3.1.1	Le rôle du NBS	52
3.1.2	L'algorithme Lucifer d'IBM	53
3.1.3	Le processus d'établissement du DES	55
3.2	L'algorithme DES	56
3.2.1	Le diagramme «en échelle»	63
3.2.2	Une représentation algébrique	64
3.3	L'effet du DES sur les données	65
3.4	Les régularités connues dans l'algorithme DES	68
3.4.1	La complémentation	68
3.4.2	Les clés faibles	69
3.4.3	Les clés semi-faibles	70

3.4.4	Les cycles hamiltoniens dans le DES	71
3.5	Les arguments sur la sécurité du DES	74
3.5.1	La recherche exhaustive d'une clé DES	74
3.5.2	Le chiffrement multiple avec le DES	76
3.5.3	Des trappes dans le DES ?	77
3.5.4	Les investigations du Sénat américain sur le DES	78
3.6	Les recherches universitaires récentes sur le DES et ses propriétés ...	78
3.7	Les mises en œuvre du DES	80
3.8	Le schéma cryptographique d'IBM	81
3.9	Le statut actuel du DES	82
Chapitre 4 L'utilisation pratique d'un chiffre par blocs		85
4.1	Les procédés d'utilisation d'un chiffre par blocs	85
4.2	Le mode « chaînage de blocs chiffrés » (CBC)	88
4.2.1	Les premier et dernier blocs	89
4.2.2	Les erreurs de transmission dans le mode CBC	91
4.2.3	Le choix de la valeur initiale	93
4.3	Le mode « rebouclage du texte chiffré » (CFB)	94
4.3.1	La propagation des erreurs dans le mode CFB	95
4.3.2	L'initialisation dans le cas du CFB	96
4.3.3	Le chiffrement d'un ensemble arbitraire de caractères	97
4.4	Le mode « rebouclage de la sortie » (OFB)	100
4.5	Les modes opératoires normalisés et non normalisés	103
4.6	Les services de sécurité dans les systèmes ouverts	105
4.6.1	La définition des services de sécurité	106
4.6.2	La place des services de sécurité dans les couches OSI	109
4.7	La place du chiffrement dans l'architecture de réseau	109
4.7.1	Le chiffrement de liaison	110
4.7.2	Le chiffrement de bout en bout	112
4.7.3	Le chiffrement nœud à nœud	114
4.7.4	Où situer le chiffrement dans l'architecture des réseaux ?	115
Chapitre 5 L'authentification et l'intégrité		117
5.1	Introduction	117
5.2	La protection contre les erreurs dans la préparation des données	119

X *Table des matières*

5.3	La protection contre les erreurs accidentelles dans la transmission des données	121
5.4	L'intégrité des données fondée sur des paramètres secrets	122
5.5	Les propriétés d'un algorithme d'authentification	124
5.5.1	L'algorithme de décalage et d'addition en décimal	126
5.5.2	L'algorithme de code d'authentification de message (MAA) ...	129
5.5.3	Les méthodes d'authentification basées sur les modes opératoires standard	131
5.6	L'intégrité des messages par chiffrement	133
5.6.1	Le choix de la méthode de contrôle de parité pour l'authentification	133
5.6.2	Le chiffrement ou l'authentification?	135
5.6.3	L'authentification sans clé secrète	135
5.7	Le problème du rejeu	136
5.7.1	L'utilisation d'un numéro de séquence de message	137
5.7.2	L'utilisation de nombres aléatoires pour l'authentification d'entité .	139
5.7.3	L'utilisation d'horodateurs	140
5.7.4	L'intégrité des données stockées	141
5.8	Le problème des litiges	143
Chapitre 6 La gestion de clés		145
6.1	Introduction	145
6.2	La génération de clé	146
6.2.1	Les générateurs de bits aléatoires	147
6.2.2	Les générateurs de nombres pseudo-aléatoires	147
6.3	Les clés de terminaux et les clés de sessions	150
6.3.1	Les chemins de distribution de la clé de session	151
6.3.2	Le protocole de distribution de clés de sessions	152
6.3.3	L'authentification pendant la phase d'acquisition de la clé	153
6.3.4	L'authentification pendant la phase de transfert	154
6.3.5	La distribution des clés de terminaux	155
6.4	Le schéma de gestion de clés d'IBM	157
6.4.1	Les conditions de la sécurité physique	157
6.4.2	La hiérarchie des clés	159
6.4.3	Le chiffrement et le déchiffrement des données dans le serveur ..	160
6.4.4	La génération et la distribution d'une clé de session	161
6.4.5	La génération et la distribution de la clé de terminal	163
6.4.6	Les principes de la sécurité des fichiers	164
6.4.7	La génération et la récupération d'une clé de fichier	165
6.4.8	Le transfert de données chiffrées entre serveurs	166

6.4.9	Le transfert de fichiers chiffrés entre serveurs	168
6.5	La gestion de clés avec étiquettes	169
6.5.1	La génération de nouvelles clés étiquetées	170
6.5.2	L'extension de la hiérarchie des clés	171
6.6	La gestion de clés pour les opérations de banque liées à l'activité de l'entreprise	172
6.6.1	La hiérarchie des clés	174
6.6.2	Le chiffrement et le déchiffrement avec des clés de longueur double	175
6.6.3	Les modes de distribution de clés et les échanges de messages ..	176
6.6.4	La distribution de clés point à point	177
6.6.5	Le centre de distribution de clés	179
6.6.6	Le centre de traduction de clés	180
6.6.7	L'utilisation consécutive de deux centres de traduction de clés ..	181
6.6.8	La notarisation et le décalage de clés	182
6.7	Les autres possibilités pour la gestion de clés	183
Chapitre 7 La vérification de l'identité		185
7.1	Introduction	185
7.2	La vérification de l'identité par la connaissance d'un élément	186
7.2.1	Les mots de passe	186
7.2.2	Les mots de passe variables basés sur une fonction à sens unique ..	192
7.2.3	Les questionnaires	193
7.3	La vérification de l'identité par la possession d'un jeton	194
7.3.1	Les cartes à pistes magnétiques	194
7.3.2	Le ruban Watermark	196
7.3.3	Le ruban sandwich	198
7.3.4	Les cartes à puce	198
7.3.5	L'authentification à l'aide d'une « calculatrice »	200
7.4	La vérification de l'identité par des caractéristiques individuelles	203
7.4.1	La reconnaissance automatique	204
7.4.2	La tolérance du système	205
7.5	La vérification de la signature manuscrite	206
7.5.1	Les techniques d'enregistrement du mouvement du stylo	207
7.5.2	L'utilisation de la vérification de signature	208
7.6	La vérification de l'empreinte digitale	208
7.7	La vérification de la voix	210
7.8	La reconnaissance de dessins rétinien	211

XII *Table des matières*

7.9	Le processus de vérification	212
7.9.1	Introduction	212
7.9.2	La vérification	213
7.9.3	Le compromis	213
7.10	L'évaluation des techniques de vérification de l'identité	217
7.10.1	Les études d'évaluation du Mitre	217
7.10.2	La voix	218
7.10.3	Les signatures	219
7.10.4	Les empreintes digitales	221
7.10.5	La comparaison des systèmes	222
7.11	Les performances d'autres systèmes de vérification de l'identité	222
7.11.1	La vérification du locuteur	222
7.11.2	La vérification de signature	224
7.11.3	La vérification d'empreinte digitale	225
7.11.4	Les dessins rétinien	225
7.11.5	La vérification du profil	226
7.12	La sélection d'un système de vérification de l'identité	226
Chapitre 8 Le chiffrement à clé publique		229
8.1	Le principe	229
8.1.1	Le contrôle d'accès avec un chiffre asymétrique	232
8.1.2	La construction d'un système à clé publique	232
8.1.3	Le retour aux fonctions à sens unique	233
8.1.4	La théorie des nombres et l'arithmétique finie	234
8.2	La fonction exponentielle et la distribution des clés	235
8.2.1	L'exponentielle comme fonction à sens unique	237
8.2.2	La complexité du logarithme	239
8.2.3	La distribution de clé	240
8.2.4	L'authentification et la transparence	243
8.3	La fonction puissance	243
8.4	Le chiffre à clé publique de Rivest, Shamir et Adleman (RSA)	247
8.4.1	Une attaque par itération et une parade	249
8.4.2	Les aspects pratiques de l'algorithme RSA	251
8.5	Le sac à dos avec trappe	257
8.6	Un algorithme basé sur les codes correcteurs d'erreurs	262
8.7	Le registre de clés publiques	264
8.8	La théorie de la complexité et la cryptographie	265

8.9	L'arithmétique finie	267
8.9.1	Le comptage en arithmétique modulo m	268
8.9.2	L'addition	268
8.9.3	La soustraction	269
8.9.4	La multiplication	269
8.9.5	La division	270
8.9.6	L'algorithme d'Euclide	271
8.9.7	Le calcul de l'inverse	272
Chapitre 9 Les signatures numériques		273
9.1	Le problème des litiges	273
9.2	Les signatures numériques utilisant un chiffre à clé publique	274
9.2.1	La combinaison de la signature et du chiffrement	277
9.2.2	Les signatures utilisant l'algorithme RSA	278
9.2.3	L'usage asymétrique du DES comme substitut à la signature ..	280
9.3	La séparation de la signature et du message	281
9.3.1	La falsification d'un message signé par la méthode des anniversaires	284
9.3.2	Les fonctions à sens unique pour la signature et l'authentification	286
9.4	Les protocoles de Fiat-Shamir pour l'identification et la signature	287
9.4.1	La base mathématique des protocoles de Fiat-Shamir	288
9.4.2	Le schéma d'identification de base	289
9.4.3	Le schéma de signature de Fiat-Shamir	291
9.5	Les signatures au moyen d'un chiffre symétrique	293
9.5.1	La méthode de signature de Rabin	294
9.5.2	Les signatures arbitrées	296
9.6	L'application pratique des signatures numériques	298
9.7	Le paradoxe des anniversaires	302
Chapitre 10 Le transfert électronique de fonds et le jeton intelligent .		305
10.1	Introduction	305
10.2	Les mécanismes de paiement traditionnels	308
10.2.1	Le chèque bancaire	308
10.2.2	Le virement	309
10.2.3	Les propriétés comparées des moyens de paiement	311
10.3	Les paiements interbancaires	312
10.3.1	La société SWIFT	313
10.3.2	Les normes de formats de messages	314

XIV *Table des matières*

10.3.3	La sécurité du système SWIFT	317
10.3.4	Le système de transfert automatisé des chambres de compensation (CHAPS)	319
10.4	Les guichets automatiques de banques	321
10.4.1	Le fonctionnement en ligne et hors ligne	323
10.4.2	La gestion du PIN	325
10.4.3	La vérification algorithmique du PIN	326
10.4.4	Le dialogue pour un GAB en ligne	328
10.4.5	Les systèmes partagés de GAB	331
10.4.6	La vérification du PIN avec un paramètre d'authentification	335
10.4.7	La cryptographie à clé publique dans un système partagé de GAB	336
10.5	Les paiements aux points de vente	337
10.5.1	La méthode de la clé de transaction	341
10.5.2	La méthode de la clé dérivée unique par transaction	344
10.5.3	Une amélioration de la méthode de la clé dérivée	347
10.5.4	Le transfert électronique de fonds aux points de vente et la cryptographie à clé publique	348
10.5.5	Les terminaux aux points de vente hors ligne et les cartes à puce	350
10.5.6	Les exigences de sécurité physique du jeton intelligent	351
10.5.7	La vérification de PIN dans le jeton intelligent	352
10.6	Le paiement par messages signés	355
10.6.1	Le paiement au point de vente par chèque électronique	357
10.6.2	Le développement du jeton intelligent	359
10.7	Le contrôle d'accès par jeton intelligent	360
10.8	Les documents négociables	363
10.8.1	Un document négociable universel	364
10.8.2	La protection des documents négociables contre le vol	367
Chapitre 11 Les normes de sécurité des données		369
11.1	Introduction	369
11.2	La normalisation et le DES	374
11.2.1	La norme fédérale FS 1027: Besoins généraux de sécurité pour des équipements utilisant le DES	376
11.2.2	Le registre d'algorithmes cryptographiques	377
11.3	Les modes opératoires	378
11.4	Le chiffrement dans la couche physique des communications de données	380
11.4.1	Les principes du chiffrement dans la couche physique	382

Table des matières XV

11.4.2	Comment signaler le début de la transmission	383
11.4.3	Le traitement d'une interruption	384
11.4.4	L'option de mise en court-circuit	385
11.4.5	Les caractéristiques du chiffrement dans la couche physique .	386
11.5	L'authentification des entités homologues	387
11.6	Les normes de sécurité des données dans le monde bancaire	389
11.7	Perspectives	390
	Bibliographie	391
	Normes françaises	399
	Liste des sigles des principaux organismes cités	402
	Glossaire	403