

RÉSEAUX
ET TÉLÉCOMS

Information – Commande – Communication

Sécurité des systèmes d'information

sous la direction de
Ludovic Mé
Yves Deswarte

 **hermes**

Lavoisier



2-005-586-1

Sécurité des systèmes d'information

sous la direction de

Ludovic Mé et Yves Deswarte

hermes
Science
— publications —

Lavoisier

Table des matières

Avant-propos	11
Ludovic MÉ et Yves DESWARTE	
Chapitre 1. Les modèles de sécurité	13
Frédéric CUPPENS et Nora CUPPENS-BOULAHIA	
1.1. Introduction	13
1.2. Contrôle d'accès	15
1.2.1. Modèle I-BAC	15
1.2.2. Modèle R-BAC	17
1.2.3. Modèle T-BAC	18
1.2.4. Modèle V-BAC	18
1.2.5. Modèle T-MAC	19
1.2.6. Modèle Or-BAC	20
1.2.7. Modèles d'autorisations dynamiques et contextuelles	22
1.2.8. Modèles d'autorisations positives et négatives	23
1.3. Contrôle de flux	25
1.3.1. Modèle de Bell et LaPadula	26
1.3.2. Modèle de non-interférence	28
1.3.3. Modèle de Bell et LaPadula étendu	29
1.3.4. Modèle de causalité	31
1.3.5. Modèles d'intégrité	32
1.3.6. Vers des modèles d'intégrité et de confidentialité : modèle DTE	33
1.4. Administration	36
1.4.1. Modèle DAC	36
1.4.2. Modèle TAM	38
1.4.3. Modèle ARBAC	39
1.4.4. Modèle AdOr-BAC	40
1.4.5. Administration dans les modèles de type MAC	40
1.5. Synthèse et perspectives	42
1.5.1. Synthèse du contrôle d'accès	42
1.5.2. Synthèse du contrôle de flux	42

1.5.3. Vers le contrôle d'usage	43
1.6. Bibliographie	44

Chapitre 2. Technologie de protection de la vie privée sur Internet 49

Yves DESWARTE et Carlos AGUILAR MELCHOR

2.1. Introduction	49
2.2. Gestion des identités	51
2.3. Communications IP anonymes	52
2.3.1. Définitions et exemples	52
2.3.2. Les MIX et les réseaux de MIX	53
2.3.3. Autres approches	57
2.4. Accès anonymes aux services	58
2.5. Autorisation préservant la vie privée	59
2.5.1. Schémas d'autorisation équilibrés	61
2.5.2. Exemples de garanties anonymes	62
2.5.3. Monnaie électronique (<i>e-Cash</i>)	64
2.6. Gestion des données personnelles	65
2.6.1. Minimisation des données personnelles	66
2.6.2. Autodétermination des données personnelles	67
2.7. Conclusion	69
2.8. Bibliographie	70

Chapitre 3. Détection d'intrusions : état de l'art, faiblesses et problèmes ouverts 73

Marc DACIER

3.1. Introduction	73
3.2. Définitions	74
3.3. Taxonomie	76
3.3.1. Paradigme de détection	77
3.3.2. Méthode de détection	78
3.3.3. Fréquence d'utilisation	82
3.3.4. Sources d'informations	83
3.3.5. Comportement après détection	84
3.4. Rappel historique	85
3.4.1. Les dix premières années	85
3.4.2. Les premiers produits	89
3.4.3. Les tendances actuelles	91
3.5. Problèmes fondamentaux	91
3.5.1. Volatilité du problème	91
3.5.2. Complexité algorithmique	92
3.5.3. Réactivité	92
3.5.4. Evaluation	93
3.6. Conclusion	93
3.7. Bibliographie	94

Chapitre 4. Les protocoles IPSec et TLS 101

Refik MOLVA

4.1. Introduction	101
4.2. Mécanismes de sécurité dans le protocole IP	102
4.2.1. Mécanisme d'authentification dans IP	104
4.2.2. Mécanisme de confidentialité dans IP	107
4.2.3. Calcul des données d'authentification	109
4.2.4. Associations de sécurité	111
4.2.5. Scénarios de déploiement d'IPsec	112
4.3. Gestion des clés	114
4.3.1. ISAKMP	116
4.3.2. Protocole Oakley	119
4.4. Sécurité dans la couche transport	121
4.4.1. La couche d'enregistrement de TLS	122
4.4.2. La couche <i>Handshake</i> de TLS	123
4.5. Conclusion	125
4.6. Bibliographie	127

Chapitre 5. Les pare-feu 129

Olivier PAUL

5.1. Introduction	129
5.1.1. Une définition des pare-feu	129
5.1.2. Un petit peu d'histoire	130
5.1.3. Le service de contrôle d'accès	132
5.2. Le contrôle d'accès au niveau réseau	133
5.2.1. Politiques de filtrage	134
5.2.2. Exemple d'implantation	146
5.3. Le contrôle d'accès au niveau circuit	147
5.3.1. Politiques de filtrage	148
5.3.2. Exemple d'implantation	159
5.4. Le contrôle d'accès au niveau applicatif	163
5.4.1. Politiques de contrôle d'accès	166
5.4.2. Exemple d'implantation	173
5.5. Architectures à base de pare-feu	177
5.5.1. Architectures simples	178
5.5.2. Architectures étendues	180
5.6. Bibliographie	184

Chapitre 6. Virus et vers informatiques 187

Eric FILIOL

6.1. Introduction	187
6.2. Définitions de base et taxonomie virale	189
6.2.1. Définitions et concepts de base	189

6.2.2. Taxonomie des infections virales	190
6.3. Les grandes fonctions virales	195
6.3.1. Diagramme fonctionnel d'un virus ou d'un ver	195
6.3.2. Modes d'infection	196
6.3.3. Virus par accompagnement de code	200
6.3.4. Techniques d'antidétection	202
6.4. La lutte antivirale	204
6.4.1. Les techniques antivirales	204
6.5. Conclusion	210
6.6. Annexe : code source du virus <i>Timid</i>	211
6.7. Bibliographie	218
Chapitre 7. Infrastructure de gestion de clés	221
ascal CHOUR	
7.1. Introduction	221
7.2. Public visé et prérequis	223
7.2.1. Ce qui est supposé connu	223
7.2.2. Ce que l'on ne trouve pas dans ce document	224
7.3. Bonnes pratiques	224
7.3.1. Contraintes réglementaires et légales	225
7.3.2. Contraintes liées aux brevets	225
7.3.3. Algorithmes et règles d'usages	226
7.3.4. Cryptopériode des clés	226
7.3.5. Contraintes sur les mécanismes de base	228
7.3.6. Résistance aux attaques	228
7.3.7. Intégrité et secret des algorithmes	230
7.3.8. Génération de clés, génération d'aléas	231
7.3.9. Séquestre, sauvegarde, restauration des clés	233
7.3.10. Séparation du rôle des clés	234
7.3.11. Architecture de clés, diversification des clés	234
7.3.12. Antirejeu	240
7.3.13. Mise à la clé	240
7.3.14. Zoom sur les infrastructures à clé publique (ICP)	242
7.3.15. Signature électronique	243
7.3.16. Aspects organisationnels	244
7.3.17. Spécification techniques d'un cryptosystème	246
7.3.18. Efficacité, conformité, confiance	247
7.3.19. Internalisation/externalisation	248
7.3.20. Points à vérifier auprès des fournisseurs	248
7.3.21. Cartes à puce	249
7.4. Conclusion	251
7.5. Bibliographie	252

Chapitre 8. Sécurité et mobilité	255
Christophe BIDAN	
8.1. Mobilité et nomadisme	256
8.1.1. Nomadisme : problèmes et solutions	256
8.1.2. Téléphonie mobile : problèmes et solutions	258
8.1.3. Mobilité dans le nomadisme	260
8.2. Sécurité	263
8.2.1. Sécurité et nomadisme	263
8.2.2. Sécurité et téléphonie mobile	268
8.2.3. Sécurité et mobilité	270
8.3. Conclusion	275
8.4. Bibliographie	276
Chapitre 9. Carte à puce	279
Jean-Louis LANET et Pierre GIRARD	
9.1. Cartes à puce et nouveaux défis	279
9.1.1. Fonctionnalités de la carte à puce	280
9.1.2. Les applications	281
9.2. Technologies de la carte à puce	283
9.2.1. Cartes à mémoire et cartes à microprocesseur	284
9.2.2. Communication entre la carte et le monde extérieur	284
9.2.3. Les cartes classiques ou « fermées »	286
9.2.4. Java Card	288
9.3. Sécurité physique	291
9.3.1. Les attaques invasives	291
9.3.2. Les attaques non invasives	292
9.4. Sécurité logique	293
9.4.1. Eviter les vulnérabilités	295
9.4.2. Méthodes formelles	295
9.4.3. Description du vérifieur	296
9.4.4. Modélisation du vérifieur	299
9.4.5. Conclusions	311
9.5. Conclusion	312
9.6. Bibliographie	313
Chapitre 10. Authentification biométrique	315
Jacek CZYZ et Luc VANDENDORPE	
10.1. Introduction	315
10.1.1. Vue d'ensemble	316
10.1.2. Authentification et identification	318
10.1.3. Biométrie et sécurité	318
10.2. Survol des principales modalités	319
10.2.1. La parole	319

10.2.2. Le visage	320
10.2.3. L'iris	320
10.2.4. Les empreintes digitales	321
10.2.5. Biométrie multimodale	323
10.3. Eléments de la théorie de la décision	324
10.3.1. Règle de décision pour l'erreur minimale	324
10.3.2. Le score	326
10.3.3. Règle de décision du risque minimal	326
10.3.4. Règle de décision du minimax	328
10.4. Evaluation des performances d'un système d'authentification	329
10.4.1. Taux de faux rejet et fausse acceptation	329
10.4.2. Courbe caractéristique	330
10.4.3. Données et protocole de validation	332
10.4.4. Intervalles de confiance	333
10.5. Conclusion	335
10.6. Bibliographie	335

Chapitre 11. Tolérance aux intrusions sur Internet 339

Yves DESWARTE, Vincent NICOMETTE, Ayda SAIDANE

11.1. La sécurité des systèmes connectés à l'Internet	339
11.1.1. Internet est vulnérable	339
11.1.2. Les techniques classiques de sécurité sont insuffisantes	341
11.2. La tolérance aux intrusions	343
11.2.1. La tolérance aux fautes	343
11.2.2. Vulnérabilités, attaques, intrusions	345
11.3. Un exemple d'architecture tolérant les intrusions : le projet DIT	347
11.3.1. Les mandataires	348
11.3.2. Les mécanismes de détection	348
11.3.3. Le gestionnaire d'alertes	352
11.3.4. La redondance adaptative : les régimes de fonctionnement	354
11.3.5. L'adaptation pour serveurs à contenu dynamique	355
11.3.6. Description d'une exécution	358
11.3.7. Discussion sur la capacité à résister aux attaques	360
11.3.8. Mesures de performance	361
11.4. Conclusion	366
11.5. Bibliographie	366