RÉSEAUX ET TÉLÉCOMS

IC2

Information – Commande – Communication

Sécurité des réseaux et systèmes répartis

sous la direction de

Yves Deswarte
Ludovic Mé

Hermes Lavoisier

Sécurité des réseaux et systèmes répartis

sous la direction de

Yves Deswarte

Ludovic Mé

Hermes Science publications

Table des matières

Avant-propos 13

Chapitre 1. La sécurité des systèmes d'information et de communication . 15
Yves DESWARTE

1.1. Introduction : définitions de la sécurité 15
1.1.1. La confidentialité. 16
1.1.2. L'intégrité 17
1.1.3. La disponibilité. 17
1.1.4. Autres facettes de la sécurité 17
1.2. Les besoins de sécurité. 19
1.3. Sécurité et sûreté de fonctionnement 20
1.4. Les attaques 22
1.4.1. Les attaquants et leurs motivations 22
1.4.2. Classification des attaques 25
1.5. Défenses 38
1.5.1. Authentification des utilisateurs. 39
1.5.2. Politiques de sécurité 41
1.5.3. Autorisation 48
1.5.4. Cryptographie. 50
1.5.5. Autres défenses. 55
1.6. Bibliographie 62

Chapitre 2. Authentification 67
Refik MOLVA et Yves ROUDIER

2.1. Introduction 67

2.1.1. Objectifs . . . 67
2.1.2. Propriétés . . . 68
2.2. Authentification faible . . . 69
2.2.1. Authentification à base d'adresse . . . 69
2.2.2. Mots de passe . . . 71
2.2.3. Mots de passe variables . . . 76
2.3. Authentification forte . . . 77
2.3.1. Génération de paramètres variables dans le temps . . . 78
2.3.2. Méthodes cryptographiques pour le calcul de la réponse . . . 83
2.3.3. Modèles de communication . . . 88
2.3.4. Protocoles avec secret partagé . . . 89
2.3.5. Protocoles à bases de clés publiques . . . 92
2.3.6. Protocoles utilisant un serveur d'authentification . . . 94
2.3.7. Dispositifs personnels . . . 96
2.4. Authentification biométrique . . . 100
2.4.1. Processus de vérification biométrique . . . 100
2.4.2. Caractéristiques biométriques . . . 101
2.4.3. Choix d'un système biométrique . . . 105
2.5. Bibliographie . . . 107

Chapitre 3. Intégrité, signature, tiers de confiance . . . 109
Pascal CHOUR

3.1. Intégrité . . . 109
3.1.1. Redondance . . . 109
3.1.2. Altération volontaire . . . 110
3.2. Signature . . . 116
3.2.1. Signature avec algorithmes symétriques . . . 117
3.2.2. Signature avec algorithmes asymétriques . . . 120
3.2.3. Erreur de mise en œuvre . . . 123
3.2.4. Erreur de construction . . . 123
3.2.5. Généralisation du système . . . 124
3.2.6. Les amis de nos amis . . . 125
3.2.7. Certification de clés . . . 126
3.2.8. Multisignatures . . . 126
3.2.9. Aspects légaux . . . 127
3.3. Tiers de confiance . . . 128
3.3.1. Considérations sur la gestion des clés . . . 128
3.3.2. Alice et Patrick créent leur TPC . . . 129
3.3.3. Histoire de quelques TPC . . . 132
3.3.4. Constitution de la TPC . . . 137
3.3.5. Aspects légaux . . . 143
3.4. Bibliographie . . . 144

Chapitre 4. Sécurité des bases de données 147
Frédéric CUPPENS

4.1. Introduction 147
4.2. Sécurité discrétionnaire 149
4.2.1. Langage d'expression des autorisations 150
4.2.2. Modification de la requête 154
4.2.3. Les fonctionnalités de SQL 155
4.3. Sécurité obligatoire 158
4.3.1. Granularité de la classification 159
4.3.2. Gestion des leurres 162
4.3.3. Inférence non autorisée d'informations 164
4.4. Bases de données statistiques 166
4.5. Architectures des bases de données multiniveaux 172
4.5.1. Approche filtre 172
4.5.2. Approche noyau de sécurité 175
4.5.3. Approche sujet de confiance 177
4.5.4. Approche réplication 178
4.5.5. Approche mixte : réplication de l'application/ partition des données 180
4.5.6. Approche distribuée 181
4.6. Conclusion 183
4.7. Bibliographie 184

Chapitre 5. Sécurité des échanges électroniques liés aux activités commerciales 187
Ludovic MÉ

5.1. Les transactions directes acheteur-vendeur 189
5.1.1. Le protocole SSL 190
5.1.2. Le protocole SET 194
5.2. Systèmes avec intermédiaires 201
5.2.1. L'argent électronique 201
5.2.2. L'intermédiation 204
5.3. Bibliographie 207

Chapitre 6. Evaluation et certification de la sécurité 209
Carlos MARTIN

6.1. Introduction 209
6.1.1. La sécurité : un besoin 209
6.1.2. La réponse : l'évaluation et la certification indépendantes 210
6.1.3. Les schémas d'évaluation et de certification 212
6.1.4. L'histoire des critères d'évaluation 215

6.2. Schéma d'évaluation et de certification 218
6.2.1. Comment se déroule une évaluation ? 218
6.2.2. La situation en France 222
6.2.3. La situation internationale 225
6.2.4. La reconnaissance mutuelle des certificats 228
6.3. Qu'est-ce qu'une évaluation selon les critères ITSEC ? 229
6.3.1. La séparation fonction-assurance 230
6.3.2. L'application aux produits et aux systèmes 230
6.3.3. La cible de sécurité 231
6.3.4. La séparation conformité-efficacité 231
6.3.5. Les preuves 232
6.3.6. Les classes de fonctionnalité 232
6.3.7. Les critères de conformité 233
6.3.8. Les critères d'efficacité 235
6.4. Qu'est-ce qu'une évaluation selon les critères communs ? 237
6.4.1. L'organisation des critères communs 237
6.4.2. L'oranisation des catalogues 237
6.4.3. Les exigences de sécurité 240
6.4.4. Le profil de protection 246
6.4.5. La cible de sécurité 247
6.4.6. L'échelle d'assurance prédéfinie 249
6.4.7. Les évaluations 252
6.5. Bilan 253
6.5.1. Le bilan des certifications 253
6.5.2. Les retours d'expérience 256
6.5.3. Les tendances 261
6.6. Bibliographie 264

Index 265