

RÉSEAUX  
ET TÉLÉCOMS

Information - Commande - Communication

**La sécurité dans les réseaux  
sans fil et mobiles 2**  
*technologies du marché*

*sous la direction de*

**Hakima Chaouchi**

**Maryline Laurent-Maknavicius**

**hermes**

*Lavoisier*

# La sécurité dans les réseaux sans fil et mobiles 2

*technologies du marché*

*sous la direction de*

Hakima Chaouchi

Maryline Laurent-Maknavicius

**Hermès**  
**Science**  
— PUBLICATIONS —

*Lavoisier*

# Table des matières

<b>Introduction</b> . . . . .	15
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
<b>Chapitre 1. Sécurité Bluetooth</b> . . . . .	19
Franck GILLET et Pars MUTAF	
1.1. Introduction . . . . .	19
1.2. La spécification Bluetooth . . . . .	22
1.2.1. Organisation des nœuds Bluetooth dans un réseau . . . . .	22
1.2.2. Architecture protocolaire d'un nœud Bluetooth . . . . .	22
1.2.3. Couche physique radio . . . . .	22
1.2.4. Bande de base . . . . .	25
1.2.5. Contrôleur de liaisons . . . . .	26
1.2.6. Adresses des périphériques Bluetooth . . . . .	27
1.2.7. Canaux logiques SCO et ACL . . . . .	28
1.2.8. Gestionnaire de liaisons . . . . .	29
1.2.9. Couche HCI . . . . .	29
1.2.10. Couche L2CAP . . . . .	31
1.2.11. Couche des services . . . . .	31
1.2.12. Profils . . . . .	33
1.3. La sécurité Bluetooth . . . . .	34
1.3.1. Modes de sécurité dans Bluetooth . . . . .	35
1.3.2. Pairage et authentification . . . . .	36
1.3.3. Chiffrement dans Bluetooth . . . . .	39
1.3.4. Attaques . . . . .	39
1.4. Conclusion . . . . .	43
1.5. Bibliographie . . . . .	44

<b>Chapitre 2. Sécurité des réseaux wi-fi . . . . .</b>	<b>45</b>
Guy PUJOLLE	
2.1. Introduction . . . . .	45
2.2. Les attaques réseau dans les réseaux sans fil . . . . .	46
2.2.1. Les attaques passives . . . . .	46
2.2.2. Les attaques actives. . . . .	47
2.2.3. L'attaque par déni de service . . . . .	47
2.2.4. Les attaques par TCP . . . . .	48
2.2.5. Les attaques par cheval de Troie . . . . .	49
2.2.6. Les attaques par dictionnaire . . . . .	49
2.3. La sécurité dans la norme 802.11 . . . . .	49
2.3.1. Les mécanismes de sécurité de 802.11 . . . . .	50
2.3.2. Le WEP ( <i>wired equivalent privacy</i> ) . . . . .	51
2.3.3. Les failles du WEP . . . . .	54
2.3.4. Une clé unique. . . . .	55
2.3.5. Les collisions d'IV . . . . .	55
2.3.6. La faiblesse du RC4 . . . . .	58
2.3.7. Les attaques . . . . .	60
2.4. La sécurité dans 802.1x . . . . .	61
2.4.1. Architecture de 802.1x . . . . .	62
2.4.2. L'authentification par port. . . . .	63
2.4.3. Déroulement d'une authentification . . . . .	63
2.5. La sécurité dans 802.11i . . . . .	64
2.5.1. L'architecture de sécurité de 802.11i . . . . .	66
2.5.2. Négociation de la politique de sécurité . . . . .	69
2.5.3. Les protocoles de sécurité radio de 802.11i. . . . .	70
2.6. L'authentification dans les réseaux sans fil . . . . .	74
2.6.1. Radius ( <i>remote authentication dial-in user server</i> ) . . . . .	74
2.6.2. Les procédures d'authentification liées à EAP . . . . .	75
2.7. Les mécanismes de sécurité de niveau 3 . . . . .	79
2.7.1. PKI ( <i>public key infrastructure</i> ) . . . . .	80
2.7.2. Les VPN de niveau 3 . . . . .	81
2.7.3. IPsec. . . . .	84
2.8. Bibliographie . . . . .	85
<b>Chapitre 3. Sécurité du Wimax . . . . .</b>	<b>87</b>
Pascal URIEN	
3.1. Introduction. . . . .	87
3.1.1. Un bref historique. . . . .	87
3.1.2. Quelques marchés. . . . .	88
3.1.3. Topologie. . . . .	89

3.1.4. Evolution de la sécurité dans les normes . . . . .	90
3.2. Couches basses du Wimax . . . . .	92
3.2.1. La couche MAC . . . . .	92
3.2.2. La couche physique . . . . .	93
3.2.3. Connexions et primitives . . . . .	94
3.2.4. Structure des trames MAC . . . . .	95
3.2.5. Les trames d'administration (management) . . . . .	96
3.2.6. Procédure de connexion d'un client dans un réseau Wimax . . . . .	96
3.3. La sécurité selon 802.16-2004. . . . .	99
3.3.1. Authentification, autorisation et distribution de clés . . . . .	100
3.3.2. Associations de sécurité . . . . .	103
3.3.3. Eléments cryptographiques . . . . .	104
3.3.4. Crypto-suites de chiffrement de la clé TEK avec KEK . . . . .	106
3.3.5. Crypto-suites de chiffrement de trames de données avec la clé TEK . . . . .	107
3.3.6. Un rapide aperçu des vulnérabilités de la norme 802.16-2004 . . . . .	107
3.4. La sécurité selon 802.16e. . . . .	109
3.4.1. Hiérarchie des clés . . . . .	111
3.4.2. Authentification de type PKMv2-RSA . . . . .	117
3.4.3. Authentification de type PKMv2-EAP . . . . .	118
3.4.4. SA-TEK 3-way Handshake . . . . .	121
3.4.5. Procédure de distribution de clés TEK . . . . .	122
3.4.6. Algorithme (optionnel) de mise à jour des clés GTEK . . . . .	123
3.4.7. Association de sécurité. . . . .	123
3.4.8. Algorithmes de chiffrement de données. . . . .	123
3.4.9. Algorithmes associés aux clés TEK . . . . .	124
3.4.10. En résumé. . . . .	124
3.5. Le rôle de la carte à puce dans les infrastructures Wimax . . . . .	124
3.6. Conclusion . . . . .	127
3.7. Glossaire . . . . .	127
3.8. Bibliographie. . . . .	129

## **Chapitre 4. Sécurité dans les réseaux mobiles de télécommunication . . . . .** 131

Jérôme HÄRRI et Christian BONNET

4.1. Introduction. . . . .	131
4.2. Signalisation . . . . .	133
4.2.1. Signalisation sémaphore 7 (SS7) . . . . .	134
4.2.2. La pile de protocole SS7. . . . .	137
4.2.3. La vulnérabilité des réseaux SS7 . . . . .	138
4.2.4. Les attaques possibles sur les réseaux SS7 . . . . .	139
4.2.5. Sécuriser SS7 . . . . .	140

4.3. Sécurité dans le monde GSM . . . . .	143
4.3.1. Architecture GSM . . . . .	144
4.3.2. Mécanismes de sécurité dans le GSM . . . . .	146
4.3.3. Lacunes sécuritaires dans l'accès radio GSM . . . . .	151
4.3.4. Lacunes sécuritaires dans la signalisation GSM . . . . .	154
4.4. Sécurité GPRS . . . . .	155
4.4.1. Architecture GPRS . . . . .	156
4.4.2. Mécanismes de sécurité GPRS . . . . .	156
4.4.3. Exploitation des failles sécuritaires du GPRS . . . . .	160
4.4.4. Sécurité applicative . . . . .	166
4.5. Sécurité 3G . . . . .	168
4.5.1. Infrastructure UMTS . . . . .	168
4.5.2. Sécurité UMTS . . . . .	169
4.6. Interconnexion des réseaux . . . . .	176
4.6.1. H.323 . . . . .	177
4.6.2. SIP . . . . .	177
4.6.3. Megaco . . . . .	177
4.7. Conclusion . . . . .	177
4.8. Bibliographie . . . . .	178
<b>Chapitre 5. Sécurité des applications téléchargées . . . . .</b>	<b>181</b>
Pierre CRÉGUT, Cuihtlauac ALVARADO et Isabelle RAVOT	
5.1. Introduction . . . . .	181
5.2. L'ouverture des terminaux . . . . .	182
5.3. Politique de sécurité . . . . .	183
5.3.1. Acteurs . . . . .	183
5.3.2. Menaces et objectifs de sécurité génériques . . . . .	184
5.3.3. Risques spécifiques à certaines catégories d'applications . . . . .	185
5.3.4. Les impacts . . . . .	187
5.3.5. Paysage réglementaire et contractuel . . . . .	188
5.4. Mise en œuvre d'une politique de sécurité . . . . .	189
5.4.1. Cycle de vie et mise en œuvre de la politique de sécurité . . . . .	189
5.4.2. <i>Trusted computing base</i> et moniteur de référence . . . . .	189
5.4.3. Répartition des mécanismes de sécurité . . . . .	190
5.5. Environnements d'exécution pour contenus actifs . . . . .	191
5.5.1. Le modèle « bac à sable » . . . . .	191
5.5.2. Systèmes sans contrôle d'exécution . . . . .	193
5.5.3. Virtualisation de la mémoire et systèmes d'exploitation ouverts . . . . .	193
5.5.4. Les environnements d'exécution de <i>bytecode</i> et les interpréteurs . . . . .	194

5.5.5. Evolution des architectures matérielles . . . . .	200
5.5.6. La protection du réseau et les solutions de DRM . . . . .	201
5.5.7. La validation des environnements d'exécution. . . . .	202
5.6. Validation des contenus actifs . . . . .	204
5.6.1. Processus de certification de contenus. . . . .	205
5.6.2. Le test des applications. . . . .	208
5.6.3. Les techniques d'analyse automatique. . . . .	209
5.6.4. La signature des contenus . . . . .	212
5.7. La détection des attaques. . . . .	214
5.7.1. La propagation des applications malveillantes . . . . .	214
5.7.2. La veille . . . . .	215
5.7.3. Les antivirus . . . . .	216
5.7.4. La gestion des terminaux à distance . . . . .	223
5.8. Conclusion . . . . .	225
5.8.1. Les directions de recherche . . . . .	225
5.8.2. Les virus et <i>malwares</i> existants. . . . .	227
5.9. Bibliographie. . . . .	228
<b>Conclusion</b> . . . . .	233
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
<b>Index</b> . . . . .	235

Le traité Information, Commande, Communication répond au besoin de disposer d'un ensemble complet des connaissances et méthodes nécessaires à la maîtrise des systèmes technologiques.

Conçu volontairement dans un esprit d'échange disciplinaire, le traité IC2 est l'état de l'art dans les domaines suivants retenus par le comité scientifique :

- Réseaux et télécoms
- Traitement du signal et de l'image
- Information et science du vivant
- Informatique et systèmes d'information
- Systèmes automatisés et productique
- Management et gestion des STICS
- Cognition et traitement de l'information.

Chaque ouvrage présente aussi bien les aspects fondamentaux qu'expérimentaux. Une classification des différents articles contenus dans chacun, une bibliographie et un index détaillé orientent le lecteur vers ses points d'intérêt immédiats : celui-ci dispose ainsi d'un guide pour ses réflexions ou pour ses choix.

Les savoirs, théories et méthodes rassemblés dans chaque ouvrage ont été choisis pour leur pertinence dans l'avancée des connaissances ou pour la qualité des résultats obtenus dans le cas d'expérimentations réelles.