

RÉSEAUX
ET TÉLÉCOMS

Information - Commande - Communication

La sécurité dans les réseaux sans fil et mobiles 1

concepts fondamentaux

sous la direction de

Hakima Chaouchi

Maryline Laurent-Maknavicius

 **hermes**

Lavoisier



La sécurité dans les réseaux sans fil et mobiles 1

concepts fondamentaux

sous la direction de

Hakima Chaouchi

Maryline Laurent-Maknavicius

Hermes
Science
— publication —

Lavoisier

Table des matières

Introduction	17
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
Chapitre 1. Introduction aux réseaux sans fil et mobiles	21
Hakima CHAOUCHI et Tara ALI YAHIYA	
1.1. Introduction	21
1.2. Réseaux mobiles cellulaires	22
1.2.1. Introduction	22
1.2.2. Fonctionnement d'un réseau cellulaire	23
1.2.2.1. L'interface radio	23
1.2.2.2. Conception des cellules	25
1.2.2.3. Ingénierie de trafic	25
1.2.2.4. Fonctionnement du système	26
1.2.3. Première génération de mobiles : 1G	28
1.2.4. Deuxième génération de mobiles : 2G	28
1.2.5. Troisième génération de mobiles : 3G	29
1.3. Réseaux sans fil IEEE 802	31
1.3.1. Introduction	31
1.3.2. WLAN : IEEE802.11	33
1.3.2.1. Architecture wi-fi	34
1.3.2.2. La couche physique	34
1.3.2.3. La couche MAC et les techniques d'accès	34
1.3.3. WPAN : IEEE 802.15	38
1.3.3.1. Bluetooth	38

1.3.3.2. UWB et Zigbee	40
1.3.4. WMAN : IEEE 802.16	41
1.3.4.1. La couche MAC	41
1.3.4.2. La couche physique	42
1.3.5. WMAN mobile : IEEE 802.20	44
1.3.6. MIH : IEEE 802.21	45
1.3.7. WRAN : IEEE 802.22	46
1.4. Réseaux mobiles Internet.	47
1.4.1. Introduction	47
1.4.2. Macromobilité	49
1.4.3. Micromobilité	51
1.4.3.1. Architectures à base de proxy	51
1.4.3.2. Architectures à base de modification de routage localisé	52
1.4.4. Mobilité personnelle et SIP	53
1.4.5. Réseaux Manet et NEMO	54
1.4.5.1. Manet.	54
1.4.5.2. NEMO	55
1.5. Les tendances actuelles	55
1.5.1. Tout IP, IMS et FMC.	55
1.5.2. B3G et 4G	56
1.5.3. Les applications	57
1.6. Conclusion	58
1.7. Bibliographie.	58
Chapitre 2. Vulnérabilités des réseaux filaires et sans fil.	61
Artur HECKER	
2.1. Introduction.	61
2.2. Sécurité dans l'ère numérique	62
2.2.1. La propriété privée : des vulnérabilités aux risques	62
2.2.2. Définition de la sécurité	64
2.2.3. Confiance et subjectivité.	66
2.2.4. La relation service-sécurité	68
2.3. Risques et menaces pour les systèmes des télécommunications	69
2.3.1. Le rôle des systèmes des télécommunications	69
2.3.2. Modèles de menaces des systèmes des télécommunications.	70
2.3.3. L'homogénéité <i>versus</i> l'hétérogénéité.	73
2.3.4. Internet et la sécurité	75
2.3.5. Le rôle du <i>medium</i>	76
2.3.6. Risques pour les infrastructures.	77

2.3.6.1. Accès illicites	77
2.3.6.2. Espionnage de l'infrastructure	77
2.3.6.3. Intrusions infrastructurelles	78
2.3.6.4. Traçabilité insuffisante	78
2.3.6.5. Indisponibilité de l'infrastructure	79
2.3.6.6. <i>Outsourcing</i>	79
2.3.7. Risques personnels	80
2.3.7.1. Accès aux données privées	80
2.3.7.2. Modification des données privées	81
2.3.7.3. Services imposteurs	81
2.3.7.4. Propriétés non contractuelles de l'accès	81
2.3.7.5. Fragilité de la plate-forme d'exécution	81
2.3.7.6. Usurpation de l'identité d'accès	81
2.4. Des vulnérabilités filaires aux vulnérabilités dans le sans-fil	82
2.4.1. Le changement de <i>medium</i>	82
2.4.2. Les terminaux sans fil	83
2.4.3. Nouveaux services	84
2.5. Conclusion	85
2.6. Bibliographie	86

Chapitre 3. Mécanismes de sécurité fondamentaux 89

Maryline LAURENT-MAKNAVICIUS, Hakima CHAOUCHI et Olivier PAUL

3.1. Introduction	89
3.2. Notions de base de la sécurité	89
3.2.1. Services de sécurité	89
3.2.2. Cryptographies symétrique et asymétrique	90
3.2.2.1. Cryptographie symétrique	91
3.2.2.2. Cryptographie asymétrique ou à clés publiques	92
3.2.2.3. Complémentarité des deux systèmes cryptographiques	94
3.2.3. Fonctions de hachage	94
3.2.4. Signatures électroniques et MAC	95
3.2.5. Infrastructure de gestion de clés (PKI) et certificats électroniques	97
3.2.5.1. Hiérarchie DNS au service d'une PKI	99
3.2.5.2. Certificats électroniques	99
3.2.5.3. Vérification de l'état non révoqué d'une clé publique	100
3.2.5.4. Problématique de l'usage des certificats électroniques aujourd'hui	101
3.2.6. Gestion de clés cryptographiques	102

3.2.7. Protocoles cryptographiques	103
3.3. Protocoles de communications sécurisées et mise en œuvre dans les VPN	106
3.3.1. <i>Secure socket layer</i> (SSL) et <i>transport layer security</i> (TLS)	106
3.3.1.1. Services de sécurité	108
3.3.1.2. Organisation de SSL en sous-couches	109
3.3.1.3. Phase d'initialisation de SSL	109
3.3.1.4. Phase de protection des données	111
3.3.1.5. Différences entre SSL et TLS	112
3.3.2. Suite de protocoles IPsec	112
3.3.2.1. Services de sécurité	113
3.3.2.2. Sous-protocoles AH et ESP	114
3.3.2.3. Protocole IKE	117
3.3.3. Comparaison des protocoles de sécurité SSL et IPsec	119
3.3.4. VPN IPsec et SSL	120
3.3.4.1. VPN IPsec	121
3.3.4.2. VPN SSL	122
3.4. Authentification	123
3.4.1. Mécanismes d'authentification	124
3.4.1.1. Authentification à base de mots de passe	125
3.4.1.2. Authentification basée sur les certificats ou PKI	126
3.4.1.3. Authentification basée sur des tickets Kerberos	127
3.4.1.4. Authentification basée sur les cartes à puce	128
3.4.1.5. Authentification basée sur la biométrie	129
3.4.2. Protocoles AAA pour contrôler l'accès à un réseau d'opérateur ou privé	130
3.4.2.1. EAP et PANA	132
3.4.2.2. Radius et Diameter	133
3.4.2.3. Centralisation de l'authentification des utilisateurs	135
3.5. Contrôle d'accès	136
3.5.1. Pare-feu	136
3.5.1.1. Taxonomie des pare-feu	137
3.5.1.2. Architectures de pare-feu	139
3.5.1.3. Combinaison avec d'autres services	140
3.5.2. Détection des intrusions	140
3.5.2.1. Taxonomie des systèmes de détection des intrusions	141
3.5.2.2. Caractérisation des attaques	143
3.6. Conclusion	144
3.7. Bibliographie	145

Chapitre 4. Mécanismes de sécurité propres au sans-fil	149
Franck VEYSSET, Laurent BUTTI et Jérôme RAZNIEWSKI	
4.1. Introduction.	149
4.2. Architecture de type <i>hotspot</i> et sécurité : les portails captifs	149
4.2.1. Présentation	149
4.2.2. Fonctionnement général d'un portail captif.	150
4.2.3. Analyse générale	151
4.2.3.1. Vue générale	151
4.2.3.2. Analyse de sécurité.	151
4.2.3.3. Améliorations possibles	153
4.2.4. Conclusion sur les technologies de portail	154
4.3. Surveiller la sécurité d'un réseau sans fil :	
la détection d'intrusion 802.11	154
4.3.1. Introduction	154
4.3.2. Architectures de détection d'intrusion 802.11	156
4.3.2.1. Architecture intégrée.	157
4.3.2.2. Architecture surcouche	157
4.3.3. Les événements perçus par la détection d'intrusion 802.11	158
4.3.4. Exemple de fonctionnement d'un logiciel de détection d'intrusion 802.11	159
4.3.5. Qualification du point d'accès illégitime	160
4.3.6. La prévention d'intrusion 802.11	161
4.3.6.1. Contre-mesures sur la voie radioélectrique.	161
4.3.6.2. Contre-mesures sur la voie filaire	162
4.3.7. La géolocalisation d'équipements 802.11.	162
4.3.8. Conclusion	163
4.4. Surveiller la sécurité d'un réseau sans fil : les leurres sur les réseaux 802.11	163
4.4.1. Introduction	163
4.4.2. Impératifs.	164
4.4.3. Mise en œuvre.	165
4.4.3.1. Configuration de la partie accès 802.11	165
4.4.3.2. Configuration de la partie émulation de réseaux et services	166
4.4.4. Résultats attendus.	166
4.4.5. Conclusion	167
4.5. Bibliographie.	167

Chapitre 5. Tatouage robuste de contenus multimédias	169
Mihai MITREA et Françoise PRÊTEUX	
5.1. Introduction.	169
5.2. Tatouage robuste : un nouvel enjeu pour la société de l’information . .	170
5.2.1. Un monde sans tatouage : quels risques ?	170
5.2.1.1. Protection des droits d’auteur	171
5.2.1.2. Contrôle automatique de flux de données multimédias	172
5.2.1.3. Multimédia enrichi	173
5.2.2. Tatouage, stéganographie et cryptage : un triptyque d’applications différenciées.	174
5.2.2.1. Tatouage <i>versus</i> stéganographie	174
5.2.2.2. Tatouage <i>versus</i> cryptage	175
5.2.3. Définitions et propriétés	175
5.2.3.1. Quantité d’information	175
5.2.3.2. Transparence	176
5.2.3.3. Robustesse	177
5.2.3.4. Probabilité de fausse alarme	177
5.2.4. Spécificités du tatouage dans le contexte de la mobilité	178
5.2.5. Conclusion	178
5.3. Des contraintes différenciées en fonction des spécificités des médias	179
5.3.1. Image fixe et vidéo : ou comment défier les pirates les plus audacieux	179
5.3.1.1. Transparence	179
5.3.1.2. Robustesse	180
5.3.1.3. Technique d’insertion	182
5.3.2. Audio : les plus grandes contraintes quant à l’imperceptibilité . .	183
5.3.2.1. Transparence	183
5.3.2.2. Robustesse	184
5.3.2.3. Technique d’insertion	186
5.3.3. Données 3D : le tatouage face à des représentations hétérogènes	188
5.3.3.1. Les surfaces NURBS	188
5.3.3.2. Représentation par images gaussiennes	189
5.3.3.3. Représentation par harmoniques sphériques	190
5.3.3.4. Représentation par carte de profondeur	191
5.3.3.5. Représentation par hologramme	192
5.3.3.6. Synthèse	192
5.4. Vers un modèle théorique de tatouage	193
5.4.1. Un cadre général : le canal de communication	193

5.4.2. Etalement de spectre <i>versus</i> information de bord	194
5.4.2.1. La méthode HIS	195
5.4.2.2. Tatouage vidéo	199
5.4.2.3. Tatouage audio	202
5.4.2.4. Tatouage d'objet 3D	203
5.4.3. Capacité du tatouage	207
5.4.4. Conclusion	209
5.5. Discussions et perspectives	210
5.5.1. Limites théoriques et avancées pratiques	210
5.5.1.1. Protection du droit d'auteur	211
5.5.1.2. Surveillance de la diffusion	212
5.5.1.3. Filature numérique (<i>forensic tracking</i>)	212
5.5.2. Tatouage et standardisation	212
5.5.2.1. Quels éléments standardiser ?	213
5.5.2.2. Etat actuel des efforts de standardisation	214
5.6. Conclusion	218
5.7. Bibliographie	219
Conclusion	225
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
Index	227

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.