

**INFORMATIQUE
ET SYSTÈMES
D'INFORMATION**

Information - Commande - Communication

Enjeux de la sécurité multimédia

sous la direction de

Touradj Ebrahimi
Franck Leprévost
Bertrand Warusfel

hermes

Lavoisier

Table des matières

Préface	15
Chapitre 1. Introduction	17
Touradj EBRAHIMI, Franck LEPRÉVOST, Bertrand WARUSFEL	
Chapitre 2. Réalités de l'espionnage électronique	19
Touradj EBRAHIMI, Franck LEPRÉVOST, Bertrand WARUSFEL	
2.1. Les origines militaires de l'espionnage électronique	20
2.2. Les moyens actuels de l'espionnage électronique au niveau international	22
2.3. La diversification des atteintes aux systèmes de traitement d'information, reflet de l'insécurité informatique	25
Chapitre 3. Introduction générale à la cryptographie et à ses applications dans la société de l'information	29
Jean-Claude ASSELBORN	
3.1. L'évolution de la cryptographie au cours du temps	30
3.1.1. La cryptographie à clé secrète	31
3.1.2. Vers de nouveaux horizons : la cryptographie à clé publique	35
3.1.2.1. L'échange de clé Diffie-Hellman	35
3.1.2.2. Le concept de cryptographie à clé publique	35
3.1.2.3. Le procédé RSA	37
3.2. <i>E-business, e-commerce et e-government</i>	38
3.3. L'intégrité et l'authenticité des documents	40
3.3.1. L'intégrité des documents	40
3.3.2. L'authenticité des documents	42
3.3.2.1. Précautions à prendre	43
3.3.2.2. Autres applications	43

3.3.2.3. Conclusion	43
3.4. La signature électronique	44
3.4.1. L'authentification du document signé et du signataire	44
3.4.2. L'identification du signataire	46
3.4.2.1. La vérification de la signature du PSC	47
3.4.2.2. La forme et le contenu des certificats	47
3.4.2.3. La validité légale de la signature électronique	47
3.4.2.4. Le problème de la révocation du certificat	48
3.4.2.5. La confiance dans le PSC	48
3.4.2.6. Le problème de la viabilité économique du PSC	49
3.4.2.7. Conclusion	50
3.5. L'horodatage	50
3.5.1. Le principe de l'horodatage	51
3.5.2. L'horodatage absolu	52
3.5.3. L'horodatage relatif	52
3.5.3.1. Conclusion	55
3.6. Anonymat et discrétion	55
3.6.1. L'anonymat des communications	56
3.6.2. La stéganographie et la discrétion des communications	57
3.6.2.1. Stéganographie sur base de textes	58
3.6.2.2. Stéganographie sur base d'images	59
3.6.2.3. Stéganographie sur base de sons	59
3.6.2.4. Conclusion	60
3.7. La protection des droits de propriété intellectuelle des œuvres multimédia	60
3.8. La monnaie électronique	61
3.9. Paiements sécurisés avec identification des partenaires	65
3.9.1. L'échange de messages entre les partenaires	67
3.9.2. L'assurance de l'authenticité et de la confidentialité	69
3.9.3. L'assurance de l'honnêteté des partenaires	71
3.10. Elections électroniques	72
3.10.1. Le procédé de vote de Chaum	73
3.10.2. Le procédé de Fujioka-Okamoto-Ohta	74
3.10.3. Conclusion	75
3.11. Conclusion	75
3.12. Bibliographie	76

**Chapitre 4. Contributions méthodologiques pour l'amélioration
de l'analyse des risques 79**
Eric DUBOIS, Nicolas MAYER, André RIFAUT, Vincent ROSENER

4.1. Introduction	79
4.2. Panorama des concepts et des approches de la gestion des risques	82
4.2.1. <i>Assets</i> et risques	82

4.2.2.	La gestion des risques	84
4.2.3.	Références en termes de normes et de méthodes	87
4.2.4.	Présentation de la méthode Ebios	88
4.2.4.1.	Introduction à la méthode	89
4.2.4.2.	Démarche	89
4.3.	Propositions d'amélioration méthodologique en matière d'analyse de risques	92
4.3.1.	D'une description textuelle à la production de modèles	93
4.3.2.	L'apport méthodologique de la démarche d'ingénierie des exigences	95
4.3.3.	L'approche décisionnelle appliquée à la conception d'une architecture	97
4.3.4.	Du caractère non séquentiel des processus d'ingénierie des exigences et d'ingénierie d'architecture	100
4.4.	Représentation et analyse formelle des <i>assets business</i> et IT	102
4.4.1.	Analyse business du domaine et des objectifs de sécurité	102
4.4.1.1.	Identification des <i>assets business</i> à l'aide des concepts <i>i*</i>	103
4.4.1.2.	Elicitation des exigences grâce aux arbres de buts	106
4.4.2.	Identification des <i>assets IT</i> et construction incrémentale de l'architecture logicielle	110
4.4.2.1.	Conception incrémentale d'une architecture	110
4.4.2.2.	Application à l'étude de cas	113
4.5.	Approche systématique et incrémentale de l'analyse de risques	117
4.5.1.	Modélisation des concepts de la gestion de risque	118
4.5.2.	Analyse de risque	119
4.5.2.1.	Ebios : étude du contexte	119
4.5.2.2.	Ebios : expression des besoins de sécurité	120
4.5.2.3.	Ebios : étude des menaces	121
4.5.2.4.	Ebios : identification des objectifs de sécurité	122
4.5.3.	Détermination des exigences de sécurité	125
4.6.	Conclusion	127
4.7.	Bibliographie	128
Chapitre 5. Cartes à puce		133
Jean-Sébastien CORON et Louis GOUBIN		
5.1.	L'invention de la carte à puce	133
5.2.	Fonctionnement d'une carte à microprocesseur	134
5.2.1.	Description physique	134
5.2.2.	Communication avec la carte	136
5.2.3.	Format logique des commandes	137
5.3.	Performances pour la signature électronique	137
5.3.1.	Multiplications et exponentiations modulaires	137
5.3.2.	Temps de calcul sur une carte à microprocesseur	138

5.4. Les attaques physiques	138
5.4.1. Classification des attaques physiques	140
5.4.1.1. Attaques invasives ou non invasives	141
5.4.1.2. Attaques actives ou passives	141
5.4.2. Attaques par injection de fautes	143
5.4.3. Attaques par analyse de consommation électrique	144
5.4.3.1. Analyse élémentaire de la consommation	145
5.4.3.2. Analyse différentielle de la consommation	146
5.4.3.3. Exemple de l'algorithme DES	146
5.5. Conclusion	148
5.6. Bibliographie	149
Chapitre 6. Reconnaissance vocale et sécurité	157
Andrzej DRYGAJLO	
6.1. Introduction	157
6.1.1. Variabilité de la voix	159
6.1.2. Dépendance au texte	159
6.1.3. Applications potentielles	160
6.2. Systèmes de reconnaissance vocale	160
6.2.1. Paramétrisation	161
6.2.2. Modélisation	161
6.2.2.1. Comparaison dynamique	162
6.2.2.2. Quantification vectorielle	163
6.2.2.3. Modèles à mélange de distributions gaussiennes	163
6.2.2.4. Modèles de Markov cachés	165
6.2.3. Classification	166
6.2.4. Décision	167
6.3. Evaluation des performances en reconnaissance vocale	168
6.4. Problèmes et limites des systèmes actuels	170
6.5. Conclusion	171
6.6. Bibliographie	171
Chapitre 7. Stéganographie	173
Touradj EBRAHIMI et Yannick MARET	
7.1. Introduction	173
7.2. Les principes fondamentaux de la stéganographie	174
7.3. Stéganographie de modèles 3D	176
7.3.1. Définitions	176
7.3.2. Principes de la méthode	177
7.3.3. Espace invariant aux transformées affines	178
7.3.3.1. Transformée inverse	180
7.3.4. Insertion du message secret	181

7.3.5. Extraction du message secret	184
7.4. Bibliographie	185
Chapitre 8. La dimension juridique de la sécurité des systèmes d'information	187
Bertrand WARUSFEL	
8.1. La complémentarité entre les aspects juridiques et techniques de la sécurité des systèmes	187
8.1.1. La technique connaît inévitablement des insuffisances face auxquelles elle a besoin du renfort du droit	188
8.1.2. La sécurité juridique des échanges et de la vie sociale impose que la technique présente une suffisante fiabilité	190
8.2. La répression des atteintes aux systèmes d'information	191
8.2.1. Les atteintes malveillantes à la sécurité des systèmes d'information	192
8.2.2. Les actes répréhensibles relatifs à la création et à la diffusion numérique de certains contenus illicites	194
8.2.3. Les nouveaux instruments de procédure pénale adaptés à la lutte contre la cybercriminalité	194
8.3. La constitution d'un droit des technologies de confiance	196
8.3.1. Les différents besoins de confiance dans une société numérisée	196
8.3.2. Les conditions de la preuve numérique et de la reconnaissance des signatures électroniques	197
8.3.3. L'importance croissante des mécanismes d'évaluation et de certification	199
8.3.4. Les restrictions à l'exportation sur les produits et technologies de cryptographie numérique	200
Index	203