

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère De L'Enseignement Supérieur Et de La Recherche Scientifique

Centre de Recherche Sur L'Information Scientifique Et Technique

Mémoire

Pour l'Obtention du Diplôme de Post Graduation Spécialisée

En

Sécurité Informatique

Thème

Les solutions de protection

des médias amovibles

Présenté par :

Mr. AHMIA Mohamed
Mr. LOUAM Djihad

Proposé et dirigé par :

Dr. TANDJAOUI Djamel,
Maitre de recherche Cerist.

Soutenu devant le jury composé de :

Dr. MEZIANE A/elkarim

Maître de recherche, Cerist.

Président du jury

Dr. ALIANE Hassina,

Maître de recherche, Cerist.

Membre

Mr. BABAKHOUYA A/alaziz,

Attaché de recherche, Cerist.

Membre

Année 2012

Sommaire

Introduction Générale	1
Chapitre I : Les différentes technologies des supports amovibles	4
I.1. La technologie des Clés USB	4
I.1.1 Principaux risques liés à l'utilisation de clés USB	6
I.2. La technologie de disque compact (CD).....	8
I.2.1 Principe de fonctionnement	9
I.2.2 Type de disques compacts	10
I.3. La technologie de DVD.....	11
I.3.1 Principes et spécificités techniques.....	12
I.3.2 Utilisation du DVD	14
I.4. La technologie du disque dur externe	15
I.4.1 Les avantages du disque dur externe.....	15
I.4.2 Les inconvénients du disque dur externe	15
I.5. Conclusion.....	16
Chapitre II : Exigences de Sécurité	17
II.1. Les services de sécurité	18
II.1.1 Confidentialité	18
II.1.2 Disponibilité	18
II.1.3 Intégrité	18
II.2. Les mécanismes de sécurité.....	19
II.2.1 La Cryptographie	19
II.2.2 L'authentification	19
II.2.3 Le contrôle d'accès	19
II.2.4 L'audit de sécurité	20
II.2.5 Les Antivirus	20
II.2.6 La protection physique.....	20
II.3. Stratégie de sécurité	21
II.3.1 Equipe chargée de la sécurité	21

II.3.1.1 RSSI.....	22
II.3.1.2 Administrateur système.....	22
III.3.2 Sensibilisation du personnel.....	22
II.4. Conclusion	24
Chapitre III : Les techniques de sécurité et les standards correspondants	25
III.1. Cryptographie.....	25
III.1.1 Cryptographie à clef secrète (symétrique)	26
III.1.2 Cryptographie à clef publique (Asymétrique)	27
III.1.3 Les fonctionnalités cryptographiques	28
III.1.4 Chiffrement par hardware	28
III.1.4.1 La clé IronKey.....	29
III.1.4.2 La clé SanDisk Cruzer Enterprise	29
III.1.5 Chiffrement par software sur le poste de travail	30
III.1.5.1 TrueCrypt.....	30
III.1.5.2 ZoneCentral.....	30
III.1.5.3 Security BOX.....	31
III.2. Les méthodes de protection contre les copies illicites	32
III.2.1 CSS (Content Scrambling System)	32
III.2.1.1 Les Clés utilisées par CSS	34
III.2.1.2 Processus du système CSS.....	35
III.2.1.3 Chiffrement des données	37
III.2.2 CPRM (Content Protection for Recordable Media)	39
III.2.2.1 C2 (Cryptomeria chiffrement).....	40
III.2.2.2 Media key block (MKB).....	41
III.2.2.3 Principe de fonctionnement CPRM.....	41
III.2.3 Les codes régionaux	43
III.3. Tatouage des données (Watermarking)	44
III.4. Conclusion.....	46
Chapitre IV : Etude comparative	47

IV.1. Analyse générale des technologies	47
IV.2. Analyse comparative.....	50
IV.3. Recommandations et solutions à envisager	51
IV.4. Liste de points à vérifier	54
IV.5. Les avantages d'utilisation sécurisée des médias amovibles.....	55
IV.6. Conclusion.....	56
Conclusion Générale	57
Bibliographie.....	58
Annexe I	60
Annexe II.....	68