

# Table des matières

<b>Introduction</b> . . . . .	1
Wiem TOUNSI	
<b>Chapitre 1. La Cyber Threat Intelligence et son évolution</b> . . . . .	3
Wiem TOUNSI	
1.1. Introduction . . . . .	3
1.2. Contexte général . . . . .	5
1.2.1. Menaces de nouvelle génération . . . . .	6
1.2.1.1. Menaces persistantes avancées ( <i>Advanced Persistent Threats, APT</i> ) . . . . .	6
1.2.1.2. Menaces polymorphes . . . . .	6
1.2.1.3. Menaces <i>zero-day</i> . . . . .	7
1.2.1.4. Menaces composites . . . . .	7
1.2.2. Structures et modèles analytiques . . . . .	8
1.2.2.1. Étapes de la perspective défensive de la <i>kill chain</i> . . . . .	8
1.2.2.2. Le modèle Diamond de l'analyse d'intrusion . . . . .	10
1.3. <i>Cyber Threat Intelligence</i> (CTI) . . . . .	11
1.3.1. Sources de la <i>Cyber Threat Intelligence</i> . . . . .	11
1.3.2. Sous-domaines de la <i>Cyber Threat Intelligence</i> . . . . .	13
1.3.3. Renseignement technique sur les menaces ( <i>Technical Threat Intelligence, TTI</i> ) . . . . .	15
1.4. Travaux connexes . . . . .	16
1.5. Problèmes de partage des renseignements sur les menaces . . . . .	18
1.5.1. Avantages du partage des renseignements sur les menaces pour l'apprentissage collectif . . . . .	18
1.5.2. Raisons de ne pas partager les renseignements sur les menaces . . . . .	19

1.6. Limites du renseignement technique sur les menaces . . . . .	23
1.6.1. La quantité avant la qualité . . . . .	23
1.6.2. Limites propres aux indicateurs de compromission (IOC) . . . . .	24
1.6.2.1. Indicateurs liés au réseau . . . . .	24
1.6.2.2. Indicateurs basés sur l'hôte : indicateurs sur les <i>malwares</i> . . . . .	26
1.6.2.3. Indicateurs liés aux courriers électroniques . . . . .	27
1.7. Bibliothèques ou plateformes de <i>Cyber Threat Intelligence</i> . . . . .	27
1.7.1. Avantages des bibliothèques de <i>Cyber Threat Intelligence</i> basées sur le <i>Cloud</i> . . . . .	28
1.7.2. Réticence à utiliser les services du <i>Cloud</i> . . . . .	29
1.8. Discussion . . . . .	29
1.8.1. L'insuffisance de partager rapidement. . . . .	29
1.8.2. Réduire la quantité de flux d'indicateurs de compromission. . . . .	30
1.8.3. Confiance dans le partage des indicateurs de compromission . . . . .	32
1.8.4. Normes pour la représentation et le partage de la <i>Cyber Threat Intelligence</i> . . . . .	34
1.8.5. Bibliothèques de <i>Cyber Threat Intelligence</i> basées sur le <i>Cloud</i> pour la connaissance collective et l'immunité . . . . .	36
1.8.5.1. Utilisation de solutions de <i>Cloud</i> privé/communautaire . . . . .	36
1.8.5.2. Être conscient des principales préoccupations en matière de sécurité sur le <i>Cloud</i> . . . . .	37
1.9. Évaluation des outils de renseignement technique sur les menaces . . . . .	38
1.9.1. Présentation des outils sélectionnés . . . . .	39
1.9.2. Discussion comparative . . . . .	40
1.10. Conclusion et travaux futurs . . . . .	42
1.11. Bibliographie . . . . .	44

## **Chapitre 2. Systèmes de gestion de la confiance : une étude rétrospective sur la confiance numérique . . . . . 53**

Reda YAICH

2.1. Introduction. . . . .	53
2.2. Définition de la confiance . . . . .	54
2.3. Genèse des systèmes de gestion de la confiance . . . . .	56
2.3.1. Modèle de contrôle d'accès . . . . .	56
2.3.2. Contrôle d'accès basé sur l'identité . . . . .	57
2.3.3. Contrôle d'accès basé sur le réseau . . . . .	59
2.3.4. Contrôle d'accès basé sur les rôles . . . . .	60
2.3.5. Contrôle d'accès basé sur l'organisation . . . . .	61
2.3.6. Contrôle d'accès basé sur les attributs. . . . .	62
2.4. Gestion de la confiance . . . . .	64

2.4.1. Définition . . . . .	64
2.4.2. Système de gestion de la confiance . . . . .	65
2.4.3. Fondations . . . . .	66
2.4.3.1. Identifiants . . . . .	66
2.4.3.2. Politiques . . . . .	68
2.4.3.3. Moteur de confiance . . . . .	70
2.4.4. Négociation automatisée de la confiance . . . . .	72
2.5. Classification des systèmes de gestion de la confiance . . . . .	73
2.5.1. Systèmes de gestion de la confiance basés sur l'autorisation . . . . .	74
2.5.2. Systèmes de gestion de la confiance basés sur les rôles . . . . .	79
2.5.3. Systèmes automatisés de négociation de la confiance . . . . .	82
2.6. Gestion de la confiance dans les infrastructures de <i>Cloud Computing</i> . . . . .	90
2.6.1. Modèles de confiance basés sur les identifiants . . . . .	91
2.6.2. Modèles de confiance basés sur les <i>Service Level Agreements</i> (SLA) . . . . .	91
2.6.3. Modèles de confiance basés sur la rétroaction . . . . .	92
2.6.4. Modèles de confiance basés sur la prévision . . . . .	93
2.7. Conclusion . . . . .	93
2.8. Bibliographie . . . . .	94

## **Chapitre 3. Risques d'attaques réseaux . . . . . 105**

Kamel KAROUI

3.1. Introduction . . . . .	105
3.2. Théorie du risque . . . . .	107
3.2.1. Définition des termes du risque . . . . .	107
3.2.2. Présentation des principales méthodes du risque . . . . .	109
3.2.2.1. EBIOS . . . . .	110
3.2.2.2. Méhari . . . . .	112
3.2.2.3. Octave . . . . .	114
3.2.3. Comparatif des principales méthodes . . . . .	115
3.3. Analyse du risque des systèmes d'information (SI) dans le contexte des réseaux informatiques . . . . .	119
3.3.1. Établissement du contexte . . . . .	119
3.3.1.1. Ressources à protéger . . . . .	119
3.3.1.2. Modèle du risque . . . . .	121
3.3.1.3. Classification du risque . . . . .	123
3.3.2. Appréciation des risques . . . . .	125
3.3.2.1. Méthode de l'alternance de bits pour l'agrégation des valeurs de criticité . . . . .	126
3.3.2.2. Appréciation de l'impact . . . . .	127
3.3.2.3. Appréciation de la probabilité d'occurrence . . . . .	129
3.3.2.4. Appréciation globale des risques . . . . .	130

3.3.3. Traitement du risque . . . . .	132
3.3.3.1. Amélioration des paramètres du risque . . . . .	132
3.3.4. Acceptation du risque . . . . .	134
3.3.5. Communication du risque . . . . .	135
3.3.6. Surveillance du risque . . . . .	136
3.4. Conclusion . . . . .	136
3.5. Bibliographie . . . . .	137

## **Chapitre 4. Aperçu analytique du flux d'informations et protection des données privées dans les systèmes Android . . . 139**

Mariem GRAA

4.1. Introduction . . . . .	140
4.2. Flux d'informations . . . . .	141
4.2.1. Flux explicites . . . . .	141
4.2.2. Flux implicites . . . . .	141
4.2.3. Canaux cachés . . . . .	142
4.3. <i>Data tainting</i> . . . . .	143
4.3.1. Approche de l'interprète . . . . .	143
4.3.2. Approche basée sur l'architecture . . . . .	144
4.3.3. Analyse statique des données taguées . . . . .	144
4.3.4. Analyse dynamique des données taguées . . . . .	145
4.4. Protection des données privées dans les systèmes Android . . . . .	147
4.4.1. Approche du contrôle d'accès . . . . .	147
4.4.1.1. Approche politique basée sur des règles . . . . .	148
4.4.1.2. Approche de prévention de l'élévation des privilèges . . . . .	149
4.4.2. Prévention des fuites de données privées . . . . .	151
4.4.2.1. Falsification des informations sensibles . . . . .	151
4.4.2.2. Analyse statique des applications Android . . . . .	152
4.4.2.3. Analyse dynamique des applications Android . . . . .	153
4.4.3. Approches des bibliothèques natives . . . . .	155
4.5. Détection des flux de contrôle . . . . .	157
4.5.1. Approches techniques du flux de contrôle . . . . .	158
4.5.2. Approches formelles du flux de contrôle . . . . .	159
4.6. Gestion des flux explicites et de contrôle en code Java et en code natif des applications Android . . . . .	161
4.6.1. Spécification formelle du problème d' <i>under-tainting</i> . . . . .	161
4.6.1.1. Définition syntaxique des connecteurs $\{\Rightarrow, \rightarrow, \leftarrow, \oplus\}$ . . . . .	162
4.6.1.2. Définition sémantique des connecteurs $\{\rightarrow, \leftarrow, \oplus\}$ . . . . .	162
4.6.2. Solution formelle du problème d' <i>under-tainting</i> . . . . .	163
4.6.2.1. Notations, définitions et théorèmes . . . . .	163

---

4.6.2.2. Preuve des règles de propagation des <i>tags</i> . . . . .	166
4.6.2.3. L'algorithme . . . . .	169
4.6.2.4. Preuve de la correction de l'algorithme. . . . .	169
4.6.2.5. Preuve de correction de <i>Dependency_Algorithm</i> . . . . .	169
4.6.2.6. Étapes de base dans <i>Dependency_Algorithm</i> . . . . .	170
4.6.2.7. Preuve de correction de <i>Set_Context_Taint</i> . . . . .	171
4.6.2.8. Preuve de correction de <i>Taint_Assigned_Variable</i> . . . . .	171
4.6.2.9. Preuve de la complétude de l'algorithme. . . . .	171
4.6.2.10. Complexité temporelle de l'algorithme . . . . .	172
4.6.3. Conception du système. . . . .	172
4.6.4. Gestion des flux explicites et de contrôle dans le code Java des applications Android . . . . .	174
4.6.4.1. Composant d'analyse statique . . . . .	174
4.6.4.2. Composant d'analyse dynamique . . . . .	175
4.6.4.3. Traitement des exceptions . . . . .	176
4.6.5. Gestion des flux explicites et de contrôle dans le code natif des applications Android . . . . .	177
4.6.5.1. Traceur d'instructions natives des <i>tags</i> . . . . .	177
4.6.5.2. Fonctions de commutation de contexte . . . . .	179
4.6.5.3. <i>Information Kernel</i> . . . . .	180
4.6.5.4. <i>Native Taint sink</i> . . . . .	180
4.6.6. Évaluation . . . . .	180
4.6.6.1. Efficacité. . . . .	181
4.6.6.2. Faux négatifs . . . . .	183
4.6.6.3. Performance . . . . .	183
4.6.6.4. Faux positifs. . . . .	184
4.6.7. Discussion . . . . .	184
4.7. Protection contre les attaques d'obfuscation de code basées sur les dépendances de contrôle dans les systèmes Android . . . . .	185
4.7.1. Définition de l'obfuscation du code . . . . .	185
4.7.2. Types d'obfuscations liés au programme . . . . .	186
4.7.3. Techniques d'obfuscation . . . . .	186
4.7.4. Obfuscation de code dans le système Android. . . . .	187
4.7.5. Modèle d'attaque . . . . .	188
4.7.6. Attaques d'obfuscation de code. . . . .	189
4.7.7. Détection d'attaques d'obfuscation de code . . . . .	191
4.7.8. Tests d'attaque d'obfuscation de code. . . . .	192
4.8. Détection d'attaques de canaux auxiliaires basées sur le <i>tag</i> des données dans les systèmes Android. . . . .	196
4.8.1. Modèle de menace cible . . . . .	197
4.8.2. Attaques dans les canaux latéraux . . . . .	198

4.8.2.1. Attaque de synchronisation . . . . .	198
4.8.2.2. Attaque de mémoire cache . . . . .	199
4.8.2.3. Attaque de pixel bitmap . . . . .	199
4.8.2.4. Attaque de métadonnées . . . . .	199
4.8.2.5. Attaque de longueur de fichier . . . . .	200
4.8.2.6. Attaque de la longueur du <i>clipboard</i> . . . . .	200
4.8.2.7. Attaque de processeur graphique . . . . .	200
4.8.3. Règles de propagation pour détecter les attaques par canal auxiliaire . . . . .	201
4.8.3.1. Règle de propagation du canal auxiliaire de synchronisation . . . . .	201
4.8.3.2. Règle de propagation du canal auxiliaire du mémoire cache . . . . .	201
4.8.3.3. Règle de propagation des métadonnées. . . . .	202
4.8.3.4. Règle de propagation GPU . . . . .	202
4.8.4. Mise en œuvre . . . . .	203
4.8.4.1. Détection d’attaques de synchronisation . . . . .	204
4.8.4.2. Détection d’attaques de mémoire cache . . . . .	204
4.8.4.3. Détection d’attaques de métadonnées. . . . .	204
4.8.4.4. Processeur graphique pour la détection d’attaques . . . . .	204
4.8.5. Évaluation . . . . .	205
4.8.5.1. Efficacité. . . . .	205
4.8.5.2. Faux positifs. . . . .	206
4.8.5.3. Performance. . . . .	206
4.9. Suivi du flux d’informations dans les approches des systèmes Android : résumé . . . . .	207
4.10. Conclusion . . . . .	212
4.11. Bibliographie . . . . .	213

<b>Liste des auteurs . . . . .</b>	<b>225</b>
------------------------------------	------------

<b>Index . . . . .</b>	<b>227</b>
------------------------	------------