
Contents

Introduction	ix
Wiem TOUNSI	
Chapter 1. What is Cyber Threat Intelligence and How is it Evolving?	1
Wiem TOUNSI	
1.1. Introduction.	1
1.2. Background.	3
1.2.1. New generation threats.	3
1.2.2. Analytical frameworks.	6
1.3. Cyber threat intelligence	9
1.3.1. Cyber threat intelligence sources.	9
1.3.2. Cyber threat intelligence sub-domains	11
1.3.3. Technical threat intelligence (TTI).	13
1.4. Related work	14
1.5. Technical threat intelligence sharing problems	16
1.5.1. Benefits of CTI sharing for collective learning	16
1.5.2. Reasons for not sharing	17
1.6. Technical threat intelligence limitations	21
1.6.1. Quantity over quality.	21
1.6.2. IOC-specific limitations	22
1.7. Cyber threat intelligent libraries or platforms.	25
1.7.1. Benefits of CTI libraries based in the cloud	26
1.7.2. Reluctance to use cloud services	26
1.8. Discussion	27
1.8.1. Sharing faster is not sufficient	27
1.8.2. Reducing the quantity of threat feeds	28

1.8.3. Trust to share threat data and to save reputation concerns	30
1.8.4. Standards for CTI representation and sharing	31
1.8.5. Cloud-based CTI libraries for collective knowledge and immunity	34
1.9. Evaluation of technical threat intelligence tools	36
1.9.1. Presentation of selected tools	37
1.9.2. Comparative discussion	38
1.10. Conclusion and future work	39
1.11. References.	40
Chapter 2. Trust Management Systems: a Retrospective Study on Digital Trust	51
Reda YAICH	
2.1. Introduction.	51
2.2. What is trust?.	52
2.3. Genesis of trust management systems	54
2.3.1. Access control model	54
2.3.2. Identity-based access control	55
2.3.3. Lattice-based access control	57
2.3.4. Role-based access control	58
2.3.5. Organization-based access control	59
2.3.6. Attribute-based access control	61
2.4. Trust management	62
2.4.1. Definition	62
2.4.2. Trust management system.	64
2.4.3. Foundations	65
2.4.4. Automated trust negotiation.	70
2.5. Classification of trust management systems.	72
2.5.1. Authorization-based TMSs	73
2.5.2. Automated trust negotiation systems	81
2.6. Trust management in cloud infrastructures	90
2.6.1. Credentials-based trust models	90
2.6.2. SLA-based trust models	90
2.6.3. Feedback-based trust models	91
2.6.4. Prediction-based trust models.	92
2.7. Conclusion	93
2.8. References	94
Chapter 3. Risk Analysis Linked to Network Attacks.	105
Kamel KAROUI	
3.1. Introduction.	105

3.2. Risk theory	107
3.2.1. Risk analysis terminology	107
3.2.2. Presentation of the main risk methods	109
3.2.3. Comparison of the main methods	116
3.3. Analysis of IS risk in the context of IT networks	120
3.3.1. Setting the context	120
3.3.2. Risk assessment	127
3.3.3. Risk treatment	133
3.3.4. Acceptance of risks	136
3.3.5. Risk communication	137
3.3.6. Risk monitoring	138
3.4. Conclusion	138
3.5. References	138

**Chapter 4. Analytical Overview on Secure Information
Flow in Android Systems: Protecting Private Data
Used by Smartphone Applications**

Chapter 4. Analytical Overview on Secure Information Flow in Android Systems: Protecting Private Data Used by Smartphone Applications	141
Mariem GRAA	
4.1. Introduction	142
4.2. Information flow	143
4.2.1. Explicit flows	143
4.2.2. Implicit flows	143
4.2.3. Covert channels	144
4.3. Data tainting	145
4.3.1. Interpreter approach	145
4.3.2. Architecture-based approach	146
4.3.3. Static taint analysis	146
4.3.4. Dynamic taint analysis	147
4.4. Protecting private data in Android systems	149
4.4.1. Access control approach	149
4.4.2. Preventing private data leakage approach	153
4.4.3. Native libraries approaches	157
4.5. Detecting control flow	160
4.5.1. Technical control flow approaches	160
4.5.2. Formal control flow approaches	162
4.6. Handling explicit and control flows in Java and native Android apps' code	164
4.6.1. Formal specification of the under-tainting problem	164
4.6.2. Formal under-tainting solution	166
4.6.3. System design	175
4.6.4. Handling explicit and control flows in Java Android apps' code	176

4.6.5. Handling explicit and control flows in native Android apps' code	180
4.6.6. Evaluation	184
4.6.7. Discussion	187
4.7. Protection against code obfuscation attacks based on control dependencies in Android systems	188
4.7.1. Code obfuscation definition	188
4.7.2. Types of program obfuscations	189
4.7.3. Obfuscation techniques	189
4.7.4. Code obfuscation in Android system	190
4.7.5. Attack model	191
4.7.6. Code obfuscation attacks	192
4.7.7. Detection of code obfuscation attacks	194
4.7.8. Obfuscation code attack tests	195
4.8. Detection of side channel attacks based on data tainting in Android systems	198
4.8.1. Target threat model	199
4.8.2. Side channel attacks	200
4.8.3. Propagation rules for detecting side channel attacks	203
4.8.4. Implementation	205
4.8.5. Evaluation	207
4.9. Tracking information flow in Android systems approaches comparison: summary	210
4.10. Conclusion and highlights	215
4.11. References	216
List of Authors	227
Index	229