

Contents

- 1 Intentional Risk and Cyber-Security: A Motivating Introduction 1**
 - 1.1 Cyber-Attacks and Cyber-Security 1
 - 1.2 A Mathematical Model for Managing Intentional Cyber-Risk 4
 - 1.3 Incorporating Game Theory to Complex Networks 6
 - 1.4 Static Risk, Dynamic Risk and New Algorithm Optimizations 7
- 2 Mathematical Foundations: Complex Networks and Graphs (A Review) 9**
 - 2.1 Introduction 9
 - 2.1.1 Complex Systems and Complex Networks 9
 - 2.1.2 Holism vs Reductionism 10
 - 2.1.3 Complex Networks and Intentional Risk 11
 - 2.2 Basic Concepts on Graphs and Networks 12
 - 2.2.1 The Origins 12
 - 2.2.2 Graphs vs Networks 14
 - 2.2.3 Matrices, Degrees, Link Density and Some Interesting Graph Families 14
 - 2.2.4 Directed and Weighted Networks 16
 - 2.2.5 Metric Structure, Connectedness, Geodesics and Some Other Concepts 18
 - 2.2.6 Characteristic Path Length, Efficiency and Vulnerability of a Network 19
 - 2.2.7 Clustering Coefficient 20
 - 2.2.8 Finding Out the Critical and the Most Influential Nodes: Eigenvector Centrality 21
 - 2.2.9 Information Flow Management: Betweenness Centrality 24
 - 2.2.10 Degree Distributions 26
 - 2.3 Some Interesting Complex Networks Models 27
 - 2.3.1 Random Networks 27
 - 2.3.2 Small-World Model 28
 - 2.3.3 Scale-Free Networks 29

2.4	New Approaches and Developments of Interest for Our Model	31
2.4.1	When Edges are More Important than Nodes: Line Graph and Related Concepts	31
2.4.2	Multilayer Networks	35
3	Random Walkers	37
3.1	An Introduction to Random Walkers	38
3.2	Different Mathematical Models of Random Walkers	43
3.3	Applications to Intentional Risk Analysis	48
3.3.1	Accessibility and PageRank	48
3.3.2	Dynamic Risk, Random Walkers and Multiplex Networks	49
4	The Role of Accessibility in the Static and Dynamic Risk Computation	53
4.1	Introduction: Edge's Accessibility and PageRank	53
4.2	Mathematical Formulation and Notation	55
4.3	Edge's PageRank via Classic PageRank	58
4.4	Edge's PageRank Through Line Graph	61
4.5	Classic PageRank vs Line-Graph's PageRank	62
5	Mathematical Model I: Static Intentional Risk	65
5.1	Intentionality Complex Network for Static Risk	65
5.2	Collapsed and Nodes and Edges Assignment Algorithms	68
5.2.1	0-Collapsed Algorithm and Anonymity Assignment	69
5.2.2	"Max-Path" Algorithm	72
5.2.3	Value Assignment Algorithm	73
5.2.4	Accessibility Assignment Algorithm	74
5.3	Static Risk Networks Construction from the Data	75
5.3.1	Intentionality Network of Users	76
5.3.2	Intentionality Network of Administrators	78
5.4	Static Risk Intentionality Network Construction Method: An Example	78
5.4.1	Construction Scheme	79
5.4.2	Description of the Method and an Example	80
5.4.3	Assignment of Attributes in the Original Network	95
5.5	Final Formula and Summary of Static Risk Model	96
6	Mathematical Model II: Dynamic Intentional Risk	99
6.1	Comparative Analysis: Static Risk vs Dynamic Risk	99
6.1.1	Accessibility in the Context of Dynamic Risk	100
6.2	Dynamic Risk Model	101
7	Towards the Implementation of the Model	103
7.1	Modeling Access	103
7.1.1	IP Source and Destination Port	103

7.1.2	IP Source (e.g. 192.168.1.105) → Destination Port (e.g. 192.168.1.250:23)	103
7.1.3	Restricted and Unrestricted Access Levels.....	104
7.1.4	Static and Dynamic Risk Access Levels	106
7.1.5	Static Risk with Network Protocol Analyzer Sniffers	106
7.1.6	Dynamic Risk with Network Vulnerability Scanners.....	106
7.2	Modeling Anonymity	108
7.3	Determining Value	108
7.4	Development of the Proof of Concept Software	108
7.4.1	Software Architecture	109
7.5	Proof of Concept	110
7.5.1	Visualization	112
7.5.2	Collapse/Expand.....	112
7.5.3	Anonymity, Accessibility and Value	112
7.5.4	Further Work for the PoC	113
References.....		121

Intentional Risk Management through Complex
Networks Analysis

Chapela, V.; Criado, R.; Moral, S.; Romance, M.

2015, XV, 126 p. 34 illus. in color., Softcover

ISBN: 978-3-319-26421-9