

Contents

List of Figures	x
List of Tables	xii
List of Algorithms	xiii
Acronyms	xiv
Glossary	xv
1. Introduction	1
1.1 Background and Introduction	2
1.2 Overview of Denial of Service Attacks.....	7
1.2.1 DoS Attacks in Real World.....	8
1.3 Security Nomenclature and Basic Concepts.....	12
1.3.1 General Security Terminology.....	12
1.3.2 Information Security Goals and Concepts.....	13
1.3.3 Denial of Service Terminology	14
1.4 Research Motivation.....	15
1.5 Research Objectives.....	18
1.6 Contributions	19
1.7 Thesis Roadmap	20
2. Availability	22
2.1 Introduction.....	23
2.2 Understanding Availability	25
2.3 Realm of Availability.....	32
2.4 Availability and Other Security Attributes.....	33
2.5 Availability and the Adversaries.....	35
2.6 Conclusion	36
3. System Level Determinants of Availability & the Impact of DoS Attacks	37
3.1 Introduction	38
3.2 Determinants	39
3.2.1 Reliability.....	39
3.2.2 Timeliness	42

3.2.3 Accessibility	44
3.3 Empirical Justification and Analysis	45
3.3.1 Experiment 1 (Validating Reliability and Timeliness)	45
3.3.1.1 Experiment Setup	45
3.3.1.2 Results and Discussion	48
3.3.1.3 Experiment Conclusion	55
3.3.2 Experiment 2 (Validating Accessibility)	56
3.3.2.1 Experiment Setup	56
3.3.2.2 Results and Discussion	57
3.3.2.3 Experiment Conclusion	63
4. Availability Metric: Design and Evaluation	64
4.1 Introduction	65
4.2 Dependability and Availability	66
4.3 Dependencies in Component Composition	68
4.4 Quantifying Dependencies	69
4.4.1 Availability Metric Design	73
4.5 Empirical Evaluation and Analysis	79
4.5.1 Experiment Setup	80
4.5.2 Results and Discussion	81
4.5.3 Conclusion	86
5. Denial-of-Service Attack	88
5.1 Introduction	89
5.2 Modes of Operation	92
5.3 Frequently Observed Attacks	95
5.3.1 UDP Flooding Attack	95
5.3.2 ICMP Flooding Attack	96
5.3.3 NTP Amplification	97
5.3.4 DNS Reflector Attack	99
5.3.5 TCP-SYN Flooding Attack	100
5.4 Conclusion	101
6. TCP-SYN Flooding: Attack Structure and Prevention	102
6.1 Introduction	103
6.2 Common Defense Mechanisms	106

6.2.1 Filtering.....	107
6.2.2 Shortening SYN-RECEIVED Timer	108
6.2.3 Increasing TCP Backlog.....	108
6.2.4 SYN Cache.....	109
6.2.5 SYN Cookies	109
6.3 Attack Prevention Mechanism.....	110
6.3.1 Related Work	110
6.3.2 Prevention Framework: Victim Based Statistical Filtering.....	111
6.3.2.1 VBSF Algorithm	113
6.4 Empirical Evaluation and Analysis	115
6.4.1 Experiment Setup.....	115
6.4.2 Results and Discussion.....	117
6.4.3 Conclusion.....	120
7. Conclusion and Future Scope	122
7.1 Conclusion Drawn	123
7.2 Recommendations for Future Work.....	126
Publications	128
References	131