List of Figures

1.1 Internet users per 100 inhabitants, world-wide 2005-2015 4
1.2 Growing number of Cyber Security Incidents reported in US and Worldwide 4
1.3 Security level and Cost 8
1.4 Peak Attack Size in the past decade 9

2.1(a) Classical CIA triad of Information Security 24
2.1(b) Modified and more realistic CIA triad of Information Security 24
2.2 A Panorama of Availability in an Organization 28
2.3 Factors that can affect Availability in an IS 28

3.1 System level determinants of Availability and the CIA triad 38
3.2 Bathtub Curve showing the failure rate of a Component in a System 40
3.3 Operating times of a Component in a System 40
3.4 Experiment 1 setup 46
3.5 TCP Handshake with zero window size 47
3.6 Available memory before the attack 49
3.7 ICMP response time before the attack 49
3.8 Memory Decay and ICMP response time, during the DoS attack 53
3.9 Memory status before and during the attack 54
3.10 ICMP response time before and during the attack 54
3.11 Experiment 2 setup 56
3.12 Run 1: Measurements of Concurrency, Availability and Response time 60
3.13 Run 1: Comparison of Availability and Response time 60
3.14 Run 2: Measurements of Concurrency, Availability and Response time 61
3.15 Run 2: Comparison of Availability and Response time 61
3.16 Run 3: Measurements of Concurrency, Availability and Response time 62
3.17 Run 3: Comparison of Availability and Response time 62

4.1 Attributes of Dependability and Security 67
4.2 Illustration of Components and their Dependencies in a System 70
4.3 Matrix Direct Dependency 71
4.4 Matrix Full Dependency 72
4.5 Experimental Setup of EES 81

4.6 Component Based Design of EES 81
4.7 Adjacency Matrix (Direct Dependency) AM_{nxn} of EES 82
4.8 Full Dependency Matrix FD_{nxn} of EES 82
4.9 Availability graph of EES components 85
4.10 Availability graph of EES System 86

5.1 A Denial-of-service attack plot 89
5.2 Distributed denial-of-service attack plot 90
5.3 5 lethal botnets in action in recent years 91
5.4 Most common Attack Structures used by DoS and DDoS 93
5.5 Steps in Coordinating a DDoS attack 94
5.6 State of UDP flooding attacks in recent years 96
5.7 The decline of ICMP flooding attacks in recent years 97
5.8 The rise of NTP Amplification attack since its inception 98
5.9 DNS amplification attack in recent years 99
5.10 State of TCP SYN flooding attack in recent years 100
5.11 Analysis of the well-known DoS attacks since 2012 101

6.1 TCP connection three-way handshake 103
6.2 TCP connection: half-open state 104
6.3 TCP SYN flooding during the half-open state and the connection request by the legitimate client 105
6.4 TTL and hosts IP address extracted from IPV4 Header 114
6.5 Destination port number extracted from the TCP Header 114
6.6 Experiment setup 116
6.7 Outline of VBS Filtering Technique 117
6.8 Port Frequency Monitoring levels 120