

Contents

1. Introduction and problem definition	1
2. Overview of worms and defense mechanism	5
2.1 Worms	5
2.2 Vulnerabilities	8
2.3 Defence mechanisms	10
2.3.1 Vulnerability signature	11
2.3.2 Signature based defense	12
3. The Proposed Vulnerability Signature Generator	14
3.1 The Modular Structure	15
3.2 Need for the merging module	18
4. The Merging module	19
4.1 CFG	19
4.2 Module architecture	20
4.3 CFG construction & GDL file generation	21
4.4 Parsing & maintenance of Data Structure	21
4.4.1 Extraction of Basic blocks	23
4.4.2 Data structure for a node of CFG	24
4.4.3 Extraction of edge information	24
4.4.4 Data structure for edge	25
4.5 What is CFG Pruning?	25
4.6 How CFG pruning help in the proposed system?	25
4.7 CFG merging	26
4.7.1 Some Important Definitions	26
4.7.2 Loop Merge	27
4.7.3 Branch Merge	32
4.7.4 Description of both the algorithms	36
5. Test Results	37
6. Conclusion & Future work	42
REFERENCES	43
APPENDIX	46