Contents

Chapter 1 Introduction 1

Chapter 2 First-Seen-SYN Filter 5

2.1 SYN Flood 5

2.2 Defending Mechanisms 7

2.3 Design and Implementation of FSS Filter 10

2.4 Analysis of FSS Filter 13

2.5 Experiments over FSS Filter 16

Chapter 3 TCP Ambiguity Scrubber Engine 21

3.1 Evasion Technique against TCP Protocol 21

3.2 Related Works in Segment Reassembly 23

3.3 The Design and Implementation of the Ambiguity Scrubber Engine 25

3.4 Experiments over the TCP Scrubber Engine 30

Chapter 4 FNP: A Pattern Matching Algorithm for Network Processor Platforms .. 34

4.1 Introductions on NIDSes and NPUs 34

4.2 Previous Pattern Matching Algorithms in NIDS 37

4.3 Design and Implementation of FNP 40

4.4 Analysis of FNP 49

4.5 Experiments over FNP 51

4.6. Summaries of FNP 60

Chapter 5 FNP^2: A MWM-like Pattern Matching Algorithm 62

5.1 Introduction of FNP^2 62

5.2 Design/Implementation of FNP^2 62

5.3 Experiments over FNP^2 64

5.4 Summaries of FNP^2 66

Chapter 6 FTSE: The FNP-Like TCAM Searching Engine 67

6.1 Introduction..67

6.2 FTSE Algorithm..68

6.3 Proposed Multiple-Pattern Matching Architecture.......................................70

6.4 Experiments of FTSE...73

Chapter 7 Conclusions 78

TSING HUA UNIVERSITY

List of Figures

Figure 1. (a) TCP Three-Way Handshaking and (b) Spoofed SYN attack ... 6

Figure 2. (a) SYN Proxy and (b) Semi-Transparent Gateway ... 8

Figure 3. The processing flow of the FSS filter. ... 12

Figure 4. FSS filter co-works with Semi-Transparent Gateway ... 13

Figure 5. Semi-Transparent Gateway works alone. ... 16

Figure 6. Test environment of FSS Filter ... 17

Figure 7. (a) Pattern occurs in packet boundary and (b) packet comes out of order ... 22

Figure 8. Attackers try to evade the NIDS by retransmitting different data. ... 22

Figure 9. The processing flow of the TCP Ambiguity Scrubber Engine ... 26

Figure 10. Proposed TCP state transition diagram ... 27

Figure 11. The flow of reassembly process ... 28

Figure 12. Processing flow for favour-new and favour-old systems ... 29

Figure 13. The setup of the experiments over the TCP Scrubber Engine ... 30

Figure 14. *PSW* Movement ... 42

Figure 15. An Example of the RST and RHT. ... 46

Figure 16. Distribution of pattern length in the current Snort ruleset ... 50

Figure 17. Number of memory accesses during pattern matching processing ... 53

Figure 18. Completion time comparison using a cache-disabled PC ... 54

Figure 19. The performance of the FNP algorithm with different packet lengths ... 58

Figure 20. Completion time comparison by using general PC with cache turned on.. 59

Figure 21. An example of the construction of *SDT* ... 64

Figure 22. Number of memory accesses during pattern matching processing ... 65

Figure 23. An example of signature layout in FTSE TCAM ... 68

Figure 24. An example of the PSW movement ... 69

TSING HUA UNIVERSITY

Figure 25. The hardware architecture of FTSE 70

Figure 26. The lookup latency could be hidden by pipelined processing.................... 72

Figure 27. Using port group to enhance throughput.. 73

清華大學
TSING HUA UNIVERSITY

List of Tables

Table I. Attacking tool’s list in the FSS Filter experiment..17

Table II. Test items in NSS TCP Segment Evasion. 31

Table III. Test items in OSEC TCP Segment Evasion. 32

Table IV. Scalability test for the FNP algorithm with randomly generated rulesets...55

Table V. The matched event rarely happens in our experiments.................................74

Table VI. The number of shift bytes are greater than 7 in over 80% cases................75

Table VII. The accuracy of the pre-filter is more than 90% in our experiment. 76

清華大學 TSING HUA UNIVERSITY