Smart Architecture for High-Speed Intrusion Detection and Prevention Systems*

Chih-Chiang Wu[1], Sung-Hua Wen[2], and Nen-Fu Huang[2,3]

[1] Computer and Communication Research Center (CCRC), National Tsing Hua University, Taiwan
[2] Institute of Communication Engineering, National Tsing Hua University, Taiwan
[3] Department of Computer Science, National Tsing Hua University, Taiwan
ccwu@cs.nthu.edu.tw

Abstract. The overall performance of an intrusion protection system depends not only on the packet header classification and pattern matching, but also on the post-operative determination of correlative patterns of matched rules. An increasing number of patterns associated with a rule heighten the importance of correlative pattern matching. This work proposes a TCAM-based smart architecture that supports both deep pattern-matching and correlative pattern-matching. The proposed architecture overcomes the difficulties in implementing TCAM when the patterns are very deep and the rules for packet payload involve many patterns whose positions lie within a range. A real case payload is simulated using a Snort 2.3 rule set and simulation results demonstrate the feasibility of the proposed architecture in supporting a high-speed and robust intrusion detection and prevention system.

1 Introduction

Signature matching is the conventional means of detecting the misuse of network protocol behavior in an intrusion detection system and intrusion prevention system (IDS/IPS), and of locating a virus in an anti-virus gateway. Most signature patterns are pre-defined strings, which reveal the presence of worms or viruses. Since various network intrusion methods have been developed, more precise signatures are required to describe the network attacks that cause a rule for packet payload to involve more patterns. We can find in Table 1, the maximum number of patterns in a rule of Snort [1], which is an open-source IDS, is increasing from version to version. In order to match a rule, these patterns should not only be matched by order but they also must be matched by a specified distance or range. Such pattern-matching is called *correlative pattern-matching*. Because the process of correlative patterns is very complicated, the performance of correlative patterns-matching becomes more and more important.

* This work was supported by MOE Program for Promoting Academic Excellent of Universities (II) under the grant number NSC-94-2752-E-007-002-PAE, and NSC project under the grant number NSC-94-2213-E007-021.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 318–328, 2006.
© Springer-Verlag Berlin Heidelberg 2006

Table 1. The trend of number of patterns in a rule

Versions	Max. number of patterns in a rule
SNORT 2.0	4
SNORT 2.1	6
SNORT 2.2	7
SNORT 2.3	9

Many memory technologies are used for storing the signature database in high-speed IDS/IPS systems. For example, DRAM is usually used for software-based pattern-matching. Although DRAM is a cost-effective solution, when gigabit throughput is required, its refresh characteristic makes it unusable. SRAM is a faster memory device, but it lacks a parallel comparison capability. As the price of Ternary Content Addressable Memory (TCAM) declines, the issue of cost becomes negligible and its parallel comparison capacity makes it more practical for using in gigabit pattern matching. Though TCAM is useful for pattern matching, cascading the TCAM is inefficient for processing deep pattern. In particular, the longest virus pattern announced in ClamAV [2] is far from the width of a single word of TCAM. Additionally, the number of patterns has grown rapidly in the past few years, and the total number of characters has also increased fast. Increasing the length of a pattern reduces the search performance of TCAM as the width of TCAM words is limited. Another problem of using a TCAM device is that only the pattern that has the highest priority is reported. Many patterns with overlapping content cannot be reported simultaneously. Therefore, a new TCAM-based structure is developed herein to overcome these issues.

In this work, a hardware-based pattern matching architecture is presented that not only improves the usage of accompanying FPGA resources when an intrusion detection system is under malicious attack but also increases the processing capacity of pattern-matching and rule-matching. This architecture supports a smart and general matching structure that can solve the problems of matching deep and large patterns and the problem of matching correlative patterns when TCAM is used. With a dedicated FPGA or ASIC, a TCAM-based coprocessor can match correlative patterns and multiple patterns, thus improving the overall performance of Network Intrusion Detection System (NIDS). The open-source Snort IDS will become the attack target of the hacker. Because its open source property, the attacker can obtain the rule database and know how to decrease the throughput of the system.

The rest of this paper is organized as follows. Section 2 reviews related works. Section 3 describes the problem of correlative pattern matching. We describe the proposed architecture in Section 4. Section 5 presents the simulation results. Finally, some conclusions are given in Section 6.

2 Related Work

Two techniques are commonly adopted on a hardware-based pattern matching. One is based on the finite state automata (FSA) [3-6], most of which