Chapter 6
Conclusions

With complicated Internet connectivity, signature-based NIDS (Network Intrusion Detection System) can not rely on the use of any one condition (payload string, regular expression, URL) to detect attack intensions. High-recognizably signatures must be included for more then one condition for a particular relationship.

With the popular open-source NIDS known as Snort, the proportion of multi-event rules which contain two or more options in the total number of rules has increased following respective software updates. In the last version (Snort 2.3, Apr, 2005), multi-event rules comprise over 1/4 of the total number of rules.

In this thesis, we translate the Snort payload rule form to (CONDITION, RELATION) pairs, which are called “events”. CONDITION contains the Snort payload keywords “*content*”, “*pcre*” and “*uricontent*” and RELATEION contains other keywords.

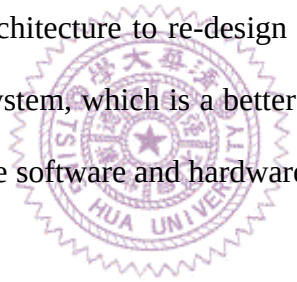
Furthermore, four important characteristics of Snort payload rules include:

1. Flow: Particular events need to check a particular network application.
2. First event: Snort utilizes the first event to classify the application.
3. Group: The first event is used to divide all rules into several independent subsets.
4. Interdependence:

   The extended event only needs to occur when the first event appears in the same group. Based on this principle, event correlation operations can be decreased.

Since multi-event rules are the trend, the Detection Engine component of Snort is critical from an efficiency perspective. We attempt a new approach to improve the Detection Engine using the above Snort rule characters. Three major aspects of this thesis include:

1. We attempt to modify the AC multi-pattern match algorithm to filter unnecessary pattern match information. This can substantially reduce the overhead of the post-processor.
2. Snort rule sets are divided into several groups. Each event needs only to search under the corresponding independent rule group. This narrows the search range and can greatly reduce the number of matches.
3. We propose a novel architecture to re-design the Snort detection engine. We propose a SoC-based system, which is a better solution because a SoC system uses both programmable software and hardware logic circuits.



We design a novel detection architecture to redesign the original Snort detection engine. We use the SoC platform (Altera's 1C20) to implement two major algorithms: EGF (event group filter) and BCRM (binary correlation match). The EGF algorithm helps us filter a lot of unnecessary information and the BCRM uses the finite state machine to find the rule ID.

The BCRM algorithm detected all attack intensions correctly. Furthermore, according to measured latency using three networks, the latency of the SoC-based system is 8~14 times faster than the pure software system.

For pure software-based systems, the event complexity is related to latency. On a SoC-based system, latency is not related to event complexity. Even with highly complex data which contains group number increases, performance will be better.

Thus, we can see that novel SoC-based NIDS solutions will coincide with future trends