Research Talk: "Performance Characterization and Improvement of SNORT"

Title: Performance Characterization and Improvement of SNORT

Speaker: Soumya Sen

Date: Thursday, August 3, 2006

ABSTRACT:

In this presentation, we will talk about our investigations towards developing an improved Intrusion Detection System (IDS), with special focus on SNORT. SNORT is an open source Intrusion Detection System which is based on the Aho-Corasick algorithm for multi-pattern search engine. It is capable of real-time packet logging, protocol analysis and content matching. Ever since the release of the first version of Snort in 2002, there has been an increasing interest among the scientific community to further improve the performance of Snort, and thereby make it suitable for keeping up with the growing security threats and network speed. Statistical data show an exponential growth in the rule sets of multi-pattern search engines. Hence it is important to find out strategies that will enable an IDS to perform well in the presence of large rule sets and on high speed networks. Our investigation into the problem has been directed at addressing these issues and identifying methods for improvement.

Apart from a general overview of Snort, we will present the modifications that have been made in the recent years to the data structures to improve memory requirements and processing speed. Results related to the performance analysis on snort based on these data structures will be provided. In addition, we will also focus on the implementation of yet another data structure (based on Jhonson's triple array and Aoe's modifications) that we have carried out and highlight the improvements it showed over Snort's multi-pattern matching engine. Lastly, an analysis of experimental results conducted on Snort using a hardware based packet generator will be given, along with a discussion about the future scope of the research work.