The Pattern Matching Algorithm Enhancement in Snort IDS

A dissertation submitted to The University of Manchester for the degree of

MSc Advanced Computer Science

in the Faculty of Engineering and Physical Sciences

2015

Siti Farhana Binti Lokman

School of Computer Science
Abstract

At the core of numerous Network Intrusion Detection System detection engines lie a critical component called multiple pattern matching algorithm. Its capability includes enabling detection engine to rapidly scan for massive amount of patterns concurrently in input packets passing through the IDS, but it is often time-consuming. Consequently, they need to be as fast as possible in order to ensure the system is scalable with high-speed networks. To avoid being vulnerable to algorithmic attacks, they need to have the capability to enforce security policies synchronously. A comprehensive overview of a number of significant pattern matching algorithms and their suitability to network IDS is provided. We deploy and compare several pattern matching algorithms with the Snort as a platform. We also introduce an algorithm added to Snort: Multi-BNDM or Multiple Backward Nondeterministic Matching, which so far has not been used in any other intrusion detection initiatives per our knowledge. Multi-BNDM which uses multiple pattern matching algorithm approach, is considered a new methodology to pattern matching in Snort.