# Abstract

Undoubtedly, the most important part of Intrusion Detection System (IDS) and firewall is the pattern-matching function to check rules. The more powerful functions and faster performance it has, the better it works in detecting intrusions. In order to handle those more complex rules for various intrusions, a powerful multi-pattern matching engine is needed not only for common rules, but also for those rules written in Regular Expression.

In this thesis, a scalable and functional custom automata system is designed. It could easily process the newly Snort rules with much smaller automata data size and overcome the disadvantages of traditional pattern-matching algorithms. Instead of processing pattern-matching, pattern-relationships, and PCRE patterns with extra CPU computing, it could save the overheads by doing those jobs in automata. The proposed automata is very suitable for hardware parallel matching engine implementation, with much less storage space and better performance.

The experiments result shows that compares with Snort system, the proposed automata system achieves perfect balance among functionality, performance, and data size. In our design, the header fields and content keywords are treated as patterns for matching, and therefore it provides an easier way to design the IDS. With this proposed core pattern-matching algorithm, various rules can be designed for complex applications.

# 中文摘要

論及網路入侵偵測系統（Intrusion Detection System）和防火牆（Firewall），其中最爲重要的關鍵即爲用來辨識與比對規則（rules）的字集比對演算法（Pattern Matching Algorithm）。倘若所使用的字集比對演算法效能越好、功能越強，整個系統在偵測各種不同的入侵行爲與處理多樣化的入侵規則時將更爲有效。爲了能夠處理現今因應日漸繁雜的入侵行爲而產生的種種複雜規則，我們需要一個不單能處理一般規則、甚至可以輕鬆處理正規語言複雜規則的強力比對引擎。

我們實作出來的特製自動機系統，融合了強大的功能性和規劃良好的規模性。它不但可以在使用了極少記憶空間的情況下輕易處理最新的 Snort 規則，更克服了傳統字集比對演算法的缺點。我們的特製自動機系統能在比對的動作中同時處理一般的字集比對、字集間的關係比對、以及由正規語言所寫的規則比對。它改進了傳統系統需花費額外的運算時間來處理此類複雜比對的缺失，同時也結合了較少的記憶體需求、較強的功能、與較佳的效能種種優點。

在本篇論文中，經由實驗測試可以發現特製自動機系統結合了功能性、效能性、與需求性三大優勢。經由我們的規劃與設計，比對各種複雜規則這件任務將可簡化爲各種字集比對的動作。這樣的設計有助於未來日益繁雜的網路環境，更能利用相同的自動機比對核心，便可處理多樣化的入侵規則。