

# Framework for Evaluation of Network-Based Intrusion Detection System

Owen Lo. Beng (Hons) Computer Networks and Distributed Systems [05002961@napier.ac.uk](mailto:05002961@napier.ac.uk)  
 Supervisor: Prof W. Buchanan. Second Marker: Dr Jamie Graves.



## 1. Introduction

In testing of IDSs, no accepted standard exists for defining the procedures or metrics of measurement for evaluation.

This project provides a methodology which takes into consideration the types of testing and metrics of evaluation required in order to assess performance of ID systems based on the dynamic nature of network traffic.

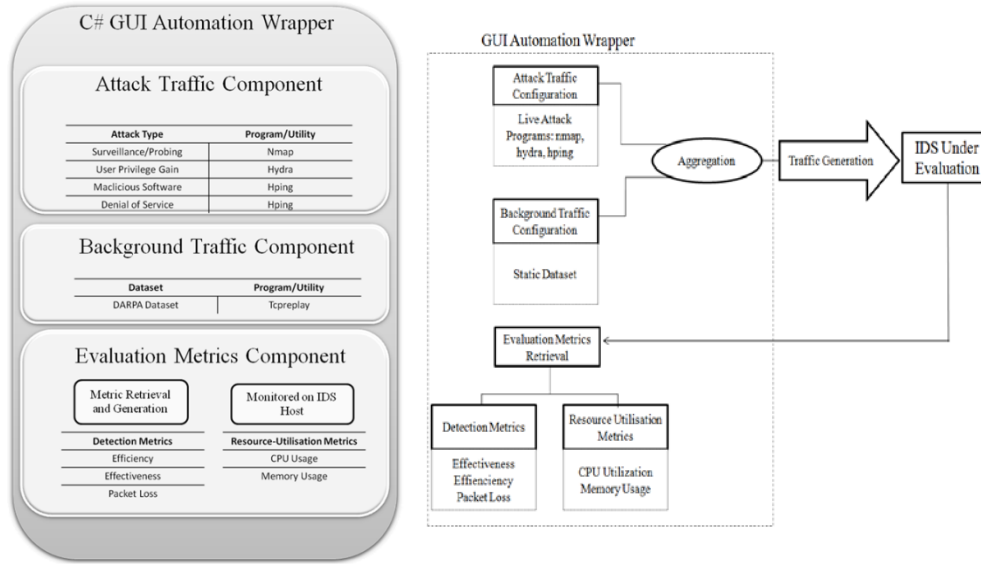
## 2. Literature Review

Research was undertaken which first provided justification for the need of security in computing. A review of the taxonomy and existing methodologies of evaluating ID systems along with the metrics of measurement which are used was then carried out. It was concluded that there are three main requirements in carrying out a effective evaluation:

- (1) **Inclusion of Realistic Attack and Benign Network Traffic**
- (2) **Ease of Automation**
- (3) **Inclusion of Meaningful Metrics for Evaluation**

## 3. Design and Methodology

A prototype framework was developed to meet all three requirements listed in the literature review. The framework and schematic is shown below:



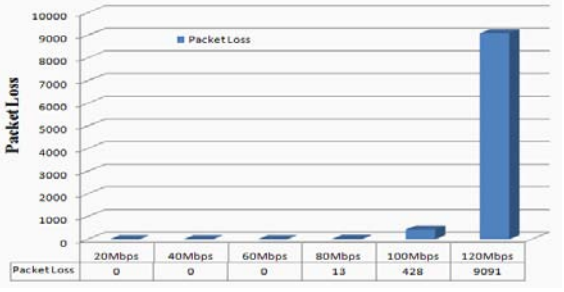
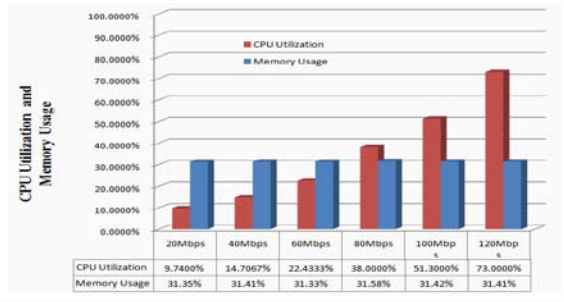
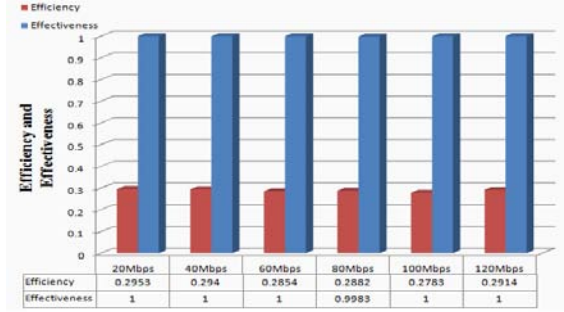
A framework was created which consists of three components: **Attack Traffic**, **Background Traffic** and **Evaluation Metrics**. The attack and background traffic component aims to meet the first criterion (realistic traffic) whilst the Evaluation Metrics component meets the third criterion. Finally, a graphical user interface was developed which wraps the three components together in order to achieve both ease of use and, more importantly, automation of testing.

## 5. Results and Conclusion



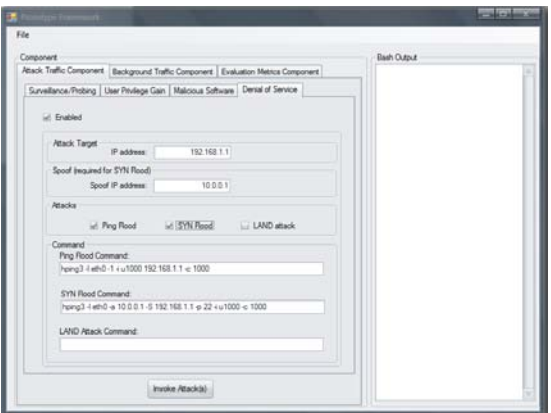
Using the framework, the evaluation was carried on the NIDS known as Snort. Snort was chosen due to it's popularity and being freely available.

Metrics of evaluation included Efficiency (True-Positive/AllAlarms), Effectiveness (True-Positive/AllPositives). Packet loss, CPU utilisation and Memory usage was also monitored.

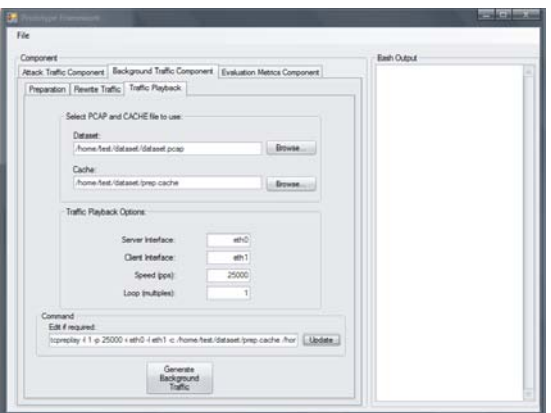


## 4. Implementation

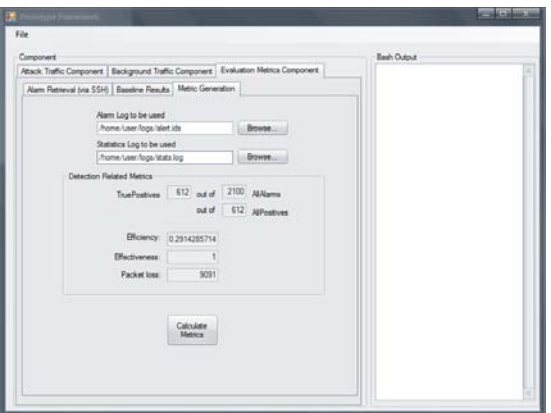
The prototype was developed using Microsoft .NET C# and runs in a Linux environment using Mono (CLR for Linux/Unix/BSD/Mac).



Attack Traffic Component



Background Traffic Component



Evaluation Metrics Component

The prototype has shown that in the evaluation of Snort, the greater the volume of network traffic the higher the CPU utilisation. This results in packet loss at  $\geq 80$ Mbps playback speeds. Furthermore, the prototype has also shown that Snort is highly effective in logging attacks but, at the same time, does raise a lot of false-positives. It was concluded that the prototype meets the initial aim of this project but further work in this area must still be carried out.