Third Year PhD Report
Online Network Intrusion Detection System Using Temporal Logic and Stream Processing

By

Abdulbasit M. Ahmed

Supervisors: Alexei Lisitsa & Clare Dixon

Advisor: Boris Konev

Submitted to

The University of Liverpool

July 3, 2011

1 Research Progress Overview

The work continued this year on the proposed research to build a Network based Intrusion Detection System using Temporal Logic (TL) and Stream Data Processing (SDP). By the end of the second year, we defined the syntax/semantics of Many Sorted First Order Metric Temporal Logic (MSFOMTL). These has been revisited and revised to have the right modeling of time. Next, the work concentrated on the mapping of the attacks which are represented in MSFOMTL into the Stream Base language. As planned, developing a misuse base NIDS with our new proposed system was the first major target. Using DARPA data and the attacks against the TCP protocol, these attacks were classified into four syntactical forms. Each of these forms can be translated automatically into an equivalent SB code that can be run on the host to detect intrusions. For syntax checking and code generation we used ANTLR (ANother Tool for Language Recognition) with Java as the target language. ANTLR is a tool that provides a framework for constructing recognizers, compilers, and translators from formal or grammatical descriptions. The paper attached to this report explain the work described above and the test results we obtained. Currently, we are conducting comparisons between our new system and other Network based Intrusion detection systems.

2 Research Plan

The descriptions of the tasks and the time plan to complete the work are as follows:

July 2011 till September 2011:

- Writing the TL to SB translation documentation.
- Building the testing data model with specified attacks.
- Generating the new IDS with these specified attacks.
- Running *BRO*, *SNORT* and our system against the testing data model and comparing the results.
- Testing scalability and performance.
- Writing a paper.

October 2011 till December 2011:

- Understanding or studying part of the TCP specification.
- Abstraction of the specs and its formal representation.
- Selecting the desired subset of TCP specs to represent.
- Experiments and results.

- Writing a paper for this approach.

January 2012 till June 2012:

- Writing Chapter 2 and 3. (10 weeks)
- Writing Chapter 4 and 5. (10 weeks)
- writing Conclusions. (5 weeks)
- Writing the Introduction. (4 weeks)

July 2012:

- Final Review and submission.

August 2012 till September 2012:

- Preparation for the VIVA.

October 2012:

- Conducting the VIVA.

3 Thesis Table Of contents

- CHAPTER 1: An Overview
  - Introduction
    - IDS Overview
    - IDS and TL
    - IDS and SB
  - Problem to Address
  - Objectives
  - Research significance
- CHAPTER 2: Temporal Logic
  - Why TL?
  - Modeling of Time
  - MSFOMTL Syntax/Semantics
  - Specification of Attacks
    - Network Packet Abstract View
    - Specifying Attacks Using MSFOMTL

    - Summary and Related Work

- CHAPTER 3: Stream Data Processing For NIDS
    - SDP Overview
    - Translation from TL into SB
    - The Proposed System
        - Design Architecture/Components
        - StreamBase and Java Adapters
        - Antlr and The Translation Process
    - Using the system as Intrusion Detection and Prevention IDPS
        - IPS Overview and General requirements
        - The Use of The New System in IDPS
    - summary and Related Work

- CHAPTER 4: Experiments and Results
    - Testing The New System
        - Building Custom Data
        - Attacks Descriptions/Representations
        - Open Source NIDS: *SNORT* and *BRO*
        - Experiments with DARPA and Custom Data Using *SNORT*, *BRO* and the new system
        - Results and Analysis of outcomes
        - Scalability and Performance
    - Summary

- CHAPTER 5: Potential Use of The new System in Anomaly IDS
    - Protocol Anomaly Overview
    - Implementing Protocol Anomaly with the new system
    - Examples of Anomaly detection in TCP
    - Experiments and Testing
    - Summary and Related Work

- CHAPTER 6: Conclusions and Future work