CSE 591 October Rotation Project Plan

Student Name	
Project Title	Adding real-time IP/TCP/UDP port usage statistics to the Passive Network Analyzer
Faculty Director	Patrick Crowley
Graduate Mentor	

Project Summary and Objective

The Passive Network Analyzer (PNA) is a real-time platform for computer network monitoring and security. The PNA platform was developed by Prof. Crowley and his students to support the rapid and low-cost development of real-time, customized network traffic monitors for use in diagnosing aberrant network traffic and, more generally, in monitoring user-specified network usage characteristics.

In this rotation project, we will develop a new real-time monitor that counts the occurrence of distinct IP/TCP/UDP port numbers in all traffic seen by the PNA device. This monitor will be used to maintain a real-time view of which network services and applications are most active in a network.

The port usage monitor will be based on an existing PNA monitor implementation, so the project activities will include a mix of learning about the PNA platform and modifying an existing monitor to observe port usage.

	Due Date	Description
Milestone 1	7-Oct	Get access to PNA source code and an account on the active node. Demonstrate a fully functioning build environment. Build and deploy the null monitor.
Milestone 2	14-Oct	Study and build the source code for the Source/Dest IP address monitor. Demonstrate the ability to modify the hash table implementation. Demonstrate ability to extract IP/TCP/UDP port numbers from incoming packets.
Milestone 3	21-Oct	Modify the Source/Dest IP address monitor to record most active ports rather than most active source IP/Ethernet MAC addresses. Test and evaluate on live network traffic.
Milestone 4	28-Oct	Capture snapshots of port usage in live traffic, varying observation periods over several days and times of day. Write a brief (2-3 page) report to report your results and summarize your experience.