Team No.: 22
Team Members:
Neel Patel
Guhyoun Nam
Steven Hu
Caleb Bryant
Kameron Bielawski

Project Name: The Watcher

Project Synopsis: Analyzing network traffic using raw sockets and delivering insights into traffic via statistics available through a GUI in multiple graphical formats.

Project Description:

The demand for traffic analysis has grown immensely in recent times. This has occurred due to the trends towards larger-scale network applications sending requests across many nodes in a data center or warehouse-scale computer. Additionally, as security concerns have increased with the information of many customers and employees being exposed across various companies, more IT professionals than ever would like insights into their internal network traffic. We propose the creation of an application to be run in a POSIX compliant OS that will utilize raw sockets to analyze network traffic and generate useful data and warnings in a GUI. The intention is for the application's output to be interpreted easily by IT professionals or any user with an interest in traffic analytics and the internals of packets being sent across the network. The value this project provides is giving users an easy way to gain at-a-glance insights into the traffic crossing their network. Graphs, charts, warnings, alerts, and other notifications are easy ways to engage a user with a GUI, and these formats make the user more likely to understand the data being presented to them.

This project has the potential to assist a wide range of professionals and hobbyists in addressing various problems. For instance, IT professionals and network administrators could discover nefarious traffic and unencrypted data being transmitted on a workplace's network. This would help protect the data of employees. Additionally, data center professionals could find the use of this application beneficial for sampling the types of traffic being sent within their fleet. When many requests are being retransmitted, this could signal an issue with a single machine and help system administrators diagnose problems.

By the end of this project, we hope to at least have a functioning traffic sampler that is capable of interpreting packets and determining their type as well as providing relevant information about the packet itself. Depending on the rate of traffic and the performance of the linux network stack as well as the hardware we are using, the traffic analyzer may be able to analyze all packets being sent across the network and give interesting analytics with the full data set. Building up a GUI is the next priority and we hope to have a usable and convenient interface for understanding the data as well as providing information about possible security concerns.

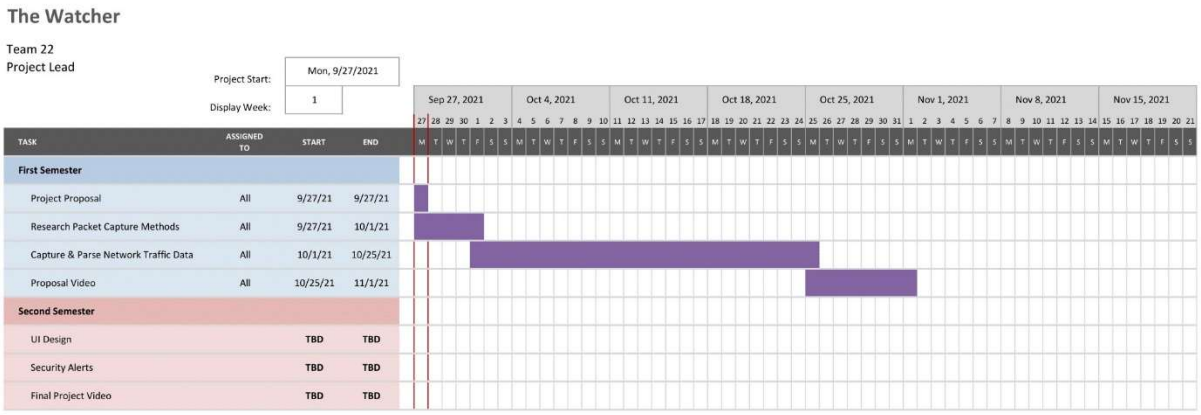
Project Milestones:

First Semester:

- Project Proposal (9/27)
- Research packet capture methods
- Be able to capture network traffic and save data into parse-able files (10/25)
- Proposal video (11/1)

Second Semester:

- Design a UI that displays info from saved data in visual format
- Integrate security alerts based on real time data
- Deliver final product and finish final project video



Project Budget:

Microsoft Azure virtual environment to capture network traffic in. Should come at no cost with Microsoft's Azure for students membership.