Interview Memorandum

To: Dr. Jaime Acosta, Mr. Christian Murga, Mr. Caesar Zapata

From: Team 5

Subject: Interview Questions for Network Traffic Proxy System

Date: 9/13/2018

CC: Elsa Tai Ramirez, Jose Cabrera Maynez

We are Team 5, consisting of Julio De La Cruz, Oscar Galindo, Kevin Gonzalez, Isai Gonzalez, and Alan Caldelas, from CS4310 Software Engineering. The purpose of this memorandum is to request an interview to Dr. Jaime Acosta, Mr. Christian Murga, and Mr. Ceasar Zapata, so that we can discuss the Network Traffic Proxy System(NTPS) project. Our team understands you are the leading expert in the project and would like to clear up any confusions or misunderstanding we have about the proposal during the interview.

All information you share about yourself or the project will be kept confidential. Only with your written permission will information be released to anyone outside of Team 5 and our instructors except as required by law. We also ask permission to record our interview for reference purposes. The interview will also be transcribed for future use.

The date of the interview will be Thursday, September 20, 7:30 am to 8:50 am in the Chemistry and Computer Science building room 1.0202. Our team representative will be asking you questions addressing a concern. After that, the class will have time to ask clarifying questions before moving on to the next concern. A list of interview questions organized by topics will be attached in the appendix.

Interview Questions

* Layering:
  + – Are the packet retransmission routines found on protocols like TCP and UDP managed by either Scapy or NFQUEUE, if not how can we suffice the requirements of the routines and succeed at intercepting packets?
  + -What are some examples of proxy utilities that currently implement hooks that we could refer to observe an example of how these snippet-functions are integrated into the system?
  + - Could you please provide a description of how a hooking mechanism functions and, if practical, provide two oral examples of scripted modifications to the intercepted packages ?
* Maintainability/Scalability:
  + -Are there any foreseeable modifications to the proxy that could help if included in the planning phase to develop a more maintainable and scalable proxy?
* Encryption:
  + -Should the proxy tool include a login/out function? If so, how should credentials be assigned?
  + -How should our proxy deal with encrypted packets, for example a collection of packets secured with SSL or TSL encryptions?
* Targeting:
  + -Should we target and “intercept” the outgoing packages of any terminal in the network by terminal name, IP address, or port?
  + -Packets that are meant to be translated from IPv6 to IPv4 should be intercepted and translated by our proxy utility ? If so, which tunneling method should we implement?
  + -Is IPv5 included in the Internet Protocols we should target? If so because of IPv5’s nature, should packages intercepted in this protocol be stored differently?
  + -When the packet intervention mode is turned off what should the proxy do with the packets it intercepted and are in the queue?
  + -It is clear you will like to see the display of all contents of, let’s say, one individual packet, but do you also want to have a filtering for just showing the headers, or just the information?
* General Implementation Questions:
  + -Would the client/professor happen to know if Linux applications have libraries that make it accessible to integrate into the system?
  + -What is Request For Comments (RFC) for?
  + -Is there any specific requirement of which language to use? Any preference between Python and C?
  + -Should the proxy be an executable application in any of the major OS (i.e. MacOS, Windows, and Linux)?
* GUI:
  + -What is the general minimum architecture that you will like to see in the GUI (please specify how its elements should interact with each other if possible) ?
  + -How should the queue of intercepted packages be displayed in the GUI?
  + -Some specific feature to include that has not been mentioned?
  + -Should we assume to include a login/out function?
  + -Should the system keep track of different user activities, if we assume more than one system analysts might use the system to keep track of different protocols?