EE/CprE/SE 491 SDMAY-19

Week 9 Report

10/7/2018 – 10/14/2018

Group number: ***5***

Project title: ***Cyber Network Capture Generator***

Client : ***Argonne National Laboratory***

Advisor : ***Benjamin Blakely***

Team Members:

Jacob Perin - ***Scribe***

Luke Tang - *Meeting Facilitator*

Collin McElvain - ***Chief Architect***

Abdelrahman Baz - ***Chief Architect***

Hazem Abdeltawab - ***Test Manager***

Bernard Ang - ***Report Manager***

Weekly Summary

This week, we had a meeting with the group and a meeting with the client. We also had a meeting with the client two week before this. In the client meeting on 10/3/2018 in Room 3138 Coover Hall at 11AM, we went over the first iteration of the Project Plan that we produced. In overall, the client and the advisor was satisfied with our Project Plan. There were some minor fixes that the client emphasized such as incorporating tasks in the risk sections and adding in security precautions. We also finalized on using Django Framework for the interface of the project. In the client meeting on 10/17/2018 in Room 3138 Coover Hall at 11AM, we went through several other risks and more details of how the program would handle certain issues. The client also suggested to look into hub concepts and setting up eht1 to broadcast and capture network. In the group meeting, tasks were delegated among the team members with Collin and Lucas working on the backend, Bernard, Abdul and Hazem working on the frontend while Jacob helps to integrate both side.

Past week accomplishments

As a team, we had a productive meeting together to further narrow down our design and tool choices for the project. We also managed to discuss in a more detailed fashion about the advantages and disadvantages of certain frameworks and tools. Each member were than tasked to work on particular parts of the project and familiarizing with each of them. The outcome of the research is shown below :

- • Bernard :
  - Researched how to create frontend using Django Framework.Django works very well with Python. It is also fast, fully loaded, scalable, versatile and secure. Worked with a tutorial to start a web page with the framework to familiarize with the framework.
  - Researched on how to create a Wireframe Diagram.
- • Jacob :
  - Researched capabilities within the Django Framework for mocking up the back end of the project. Promising capabilities for modeling objects and generating a dummy database with PCAP data.
  - Performed project feasibility research. Looked into new technologies to fill in voids and updated project structure. For e.g., XAPI and XenServer are not great options. XenServer is feature heavy, but is more so for organizations and not specialized operations. XAPI is deprecated, kind of. Through research I found a better build that will emphasize the clients needs for configuration management and makes use of modern, in-use tools.
  - Began setup on lab machines. Netbooted proper build of Ubuntu 18.04 and Xen Hypervisor 4.9. This will ensure up-to-date use for as long as possible.
- • Collin :
  - Researched Chef and Vagrant. This seems to be our solution for initializing and configuring our VM's. We will initialize the VM using vagrant as well as initializing the connection to Chef server. Each of the VM's will have a chef client, making it a node in the Chef server side. This will allow for easy distribution of applications and configurations through chef cookbooks.
  - Began download and setup on new machines
- • Lucas:
  - Finalized software dependencies: we will be using Django framework, Vagrant, Chef, Xen loaded with Ubuntu which comes with Libvirt. Also looked into capturing PCAP data. Network traces can be captured on the VM VIF, Virtual bridge, and PIF.
- •Abdelrahman:
  - Researched Django framework and what can we achieve using it. It looks promising for easing the process of creating our web app plus it is free and

open-source.

  - ➢ Started experimenting with Django framework, as we decided to use it for front end development. It includes a lightweight web server that we can use for testing. Also, Django can fake a backend database which will be helpful during the development process.

- ❖ • Hazem :
  - ➢ This week, the plan has changed. I ended up researching Django in order to start working on the project front end. Bernard, ambaz and I will all be working on the front end, using Django framework.

Individual contributions

Team member	**Contribution**	**Weekly Hours**	**Cumulative Hours**
Bernard Ang	Researched on how to create frontend with Django	**6**	**13+6 = 19**
Collin Mcelvain	Configuration management, and setup on new machines.	**5**	**13+5=18**
Jacob Perin	Project feasibility research, Partial Project Setup, Django Framework research	**8**	**13 + 8 = 21**
Lucas Tang	Finalize software dependencies upon group research and collusion	**6**	**13 + 6 = 19**
Abdelrahman Baz	Researched and experimented on Django framework	**8**	**12 + 8 = 20**
Hazem Abdeltawab	Research and practice Django Framework	**8**	**21 + 8 = 29**

Plan to accomplish for the next week

- ❖ Bernard
  - ➢ Being able to explain how the Django Framework works and how it can be integrated with our projects.
  - ➢ Draw out the Wireframe diagram for each interface.
- ❖ Collin

    - Testing on machines of vagrant and chef server. Began the creation of multiple VM's with vagrantFile's and configuration cookbooks in Xen.
- Jacob
    - Team meetings after adequate research to discuss initial findings and make decisions on specific server, framework, and server setup. Plan to diverge team into two halves (communicating for eventual re-merge) to develop project faster.
    - Assist Collin and Luke with tool stack research.
    - Perform Django research and speak with front end developers.
- Hazem
    - Do more intensive testing using Django. At least get one prototype running.
- Abdelrahman
    - Get more familiar with Django by developing several web apps.
    - Find out how Django is used to mock up the backend
- Luke
    - Research ISEAGE and its counterparts to use as a proxy to the network.
    - Begin set up stages for Virtual environment on the given hardware machines.
    - Bridge the network for our machines