June/July Progress Report

Since the end of the June exams I have accomplished the following

1. Finished and submitted ISSA paper
2. Developed a dashboard framework
3. Planned and outlined a short (8 page) paper on network telescopes with a focus on my dashboard and active/passive traffic.

1. ISSA Paper, Virtual honeypot analysis and tarpit investigation

Not to much to say about the paper, it has been finished and submitted to ISSA. There are definite sections in the paper that I will be referencing in my final thesis.

2. Development of dashboard framework

The development of the dashboard framework is essentially done, the only thing left to do is iron out the last few kinks and make adjustments to improve it. I've decided to nickname my dashboard framework as "Ember". The dashboard was made to display information obtained from the analysis of network telescope data, the information lingers in the dashboard just as heat remains in embers after a fire and so the name was chosen. Allot of planning and revision was done to come up with this framework. At first it seemed as if it would be a quick project but once I decided to make a dynamic framework that could be re-used easily create other dashboards it was evident that allot of thought would have to go into it. Here follows a brief explanation of the structure of the dashboard framework.

High Level Overview

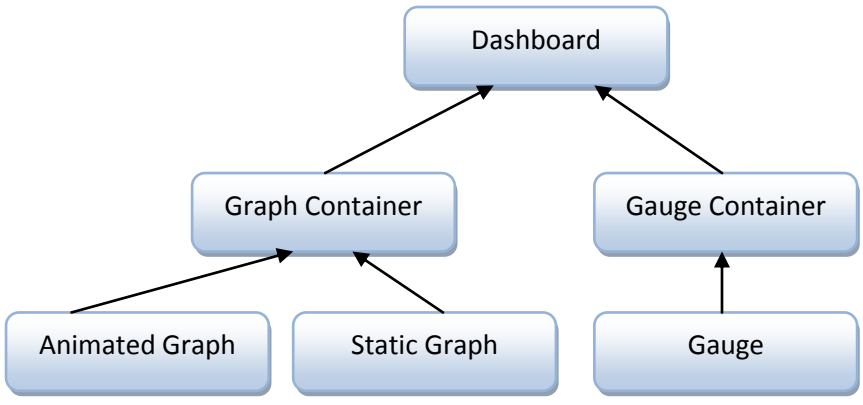
The overview begins by explaining the structure of the dashboard and the capabilities of the container object. I will then explain the functionality of the code and provide an example of the directory structure used for the framework.

The Dashboard contains multiple containers.

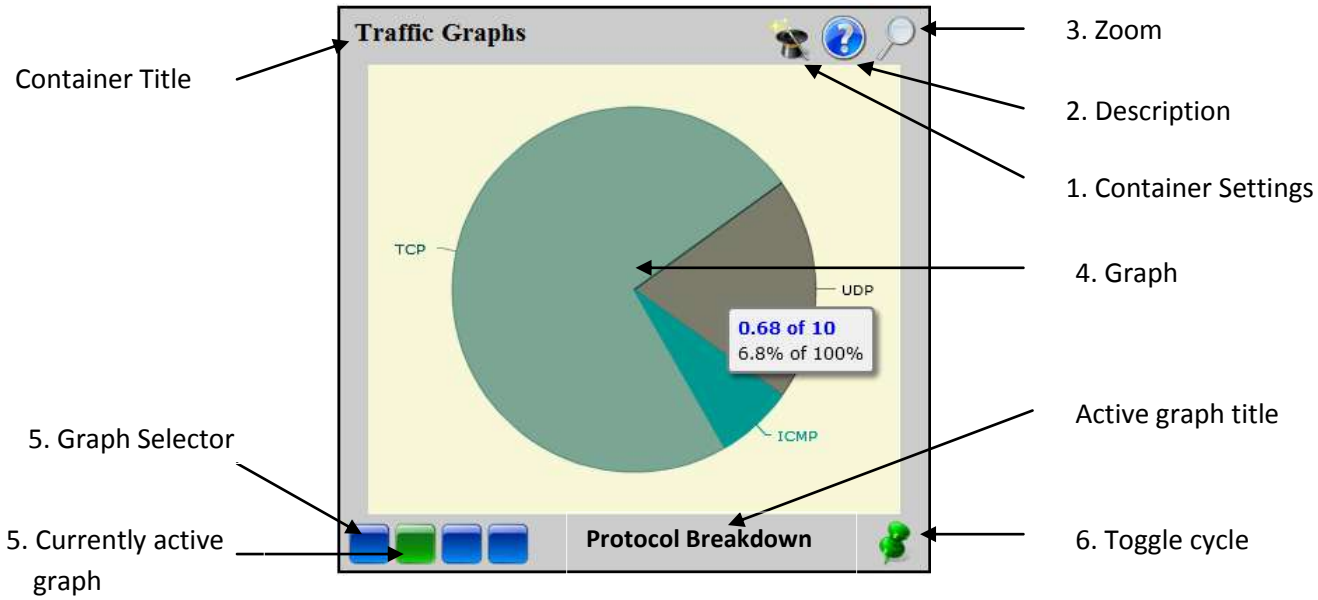
Each container consists of multiple graphs or gauges.

Graphs are either static or animated (animated means they change over time)

All containers have the ability to cycle through their graphs at a set time interval



Furthermore, each Container has the following abilities (with the exception of the Gauge container):



1. Change settings of the container (which graphs should be displayed, time interval for graph cycle)
2. View description of active graph
3. Zoom (full-screen currently active graph)
4. Graph
5. Select a graph to be active (displayed in the container)
6. Toggle graph cycle

A dashboard can contain multiple containers and each container multiple graphs, static graphs like the pie chart above to not change. However animated graphs do exist, such as a line chart that is drawn as time is elapsed or the gauges that move over time.

Code Explanation & Directory structure

There are 3 main files that form the core of the dashboard framework

- DashGen.php
  - Constructs all the html & javascript that generates the dashboard in a browser
- XMLConstructor.php
  - Parses the dashboard configuration file and helps construct the objects used by DashGen.php
- DashConfig.xml
  - Contains the following information used to construct the dashboard, an example of the configuration file is given below.

```
<dashboard title="Dashboard of Awesomeness">
    <containers num="1">
        <container title="container 1 for DashGen" cid="cont1" numgraphs="1">
            <graph active="true" php_script_location="graphScript.php" />
        </container>
    </containers>
</dashboard>
```

There is also a 4th type of file that is crucial to the dashboard, namely the graph scripts. These php scripts contain all the details of a respective graph and produce a formatted string that is used by the flash SWF object to draw the graph. The graph scripts are placed in folders grouping them by container which is found in the graph_scripts folder. Below is an illustrated example of the dashboard framework's file structure, (f) indicates a folder.

- (f)Ember
    - DashGen.php
    - XMLConstructor.php
    - DashConfig.xml
    - (f)Images
        - <images used in dashboard>
    - (f)Libraries
        - (f)openflash
            - <openflash chart 2 library files>
    - (f)Style
        - Cascading Style Sheets (css)
    - (f)Graph_scripts
        - Geo_Analysis
            - <graphscripts.php>
        - Protocol Analysis
            - <graphscripts.php>
        - TopN_Analysis
            - <graphscripts.php>
        - Traffic_Analysis
            - <graphscripts.php>

The following still needs to be implemented:

1. Gauges & Gauge Container
2. Graph Settings (trivial, will rewrite xml)
3. Geographic Graphs
4. Zoom function (trivial, have code just haven't implemented yet)

3. Network Telescope Dashboard short paper

I've planned the paper and written about 2 pages so far, below I've included only the rough structure.

A Network Telescope Information Framework

1. Abstract

2. Introduction

3. Backscatter: active and passive traffic

3.1 Assumptions

3.2 The architecture of the internet (nothing is certain, routing is messed up, intro to malicious users)

3.3 Malicious users (include ip spoofing and infer filtering)

3.4 Bandwidth and processing constraint (we don't get the whole picture)

4. Metrics and Information Dashboards

4.1 Metrics

4.2 I Dashboard Considerations

- network telescopes
- Backscatter
    - automated worm propagation
    - Denial of Service attacks
    - noise
- information dashboards
- security metrics
- data visualisation

5. Research outcome

- requirements
- what it will accomplish
- problems faced
    - inferring things
    - processing time of querying a large database
    - information overload
- how to overcome these problems
- what new fields of research does it open?
- how this can benefit us

6. Implementation

- Design specs
- diagrams
- architecture
- befits of doing it this way

- end result

7. Future extensions

- Mash-ups with:
    - Google earth
    - honeypots (email)
    - IDS
    - other network telescopes
    - exporting files for use in Microsoft pivot and other data mining tools

8. Conclusion

Second Semester Plan of Action

What needs to be done

- Development needs to be finished (as explained in the beginning of the report)
- User study (Usability testing)
- Write up
- Other Work
    - ISSA presentation
    - Short Paper

Week	**Work**
1-3	Finish Development
	ISSA Presentation
4-6	User Testing and Fine Tuning, short paper
7	User Testing write-up, short paper
8	Finish Short Paper
9-13	Finish Write-up