

# Weekly Report

Student: Christopher Schwagele

Week Number 21 on 19 July 2010

## Summary of activities since last meeting

### Week 1:

- Readings for Literature Review
- Literature Review

### Week 2:

- Modified the InetVis port to use separate threads to capture packets and to process openGL plotting. - Looked into reading from pcap files and storing to pcap files

### Week 3:

- Researched using the pInvoke method call to call unmanaged dll methods from within the .Net framework.
- Decided to stop the port of the openGL component and rather start with a fresh implementation using the openGL control provided by openTK.

### Week 4:

- Went to East London

### Week 5:

- Tried to create an MDI application which was the initial plan for InetVis but had problems with getting the glComponent to draw. Experimented with other possibilities such as running a separate game window instead of an embedded child form on the isolated thread.

### Week 6:

- Looked into an XNA implementation rather than the openGL counterpart. XNA provides better functionality than the openTK openGL wrapper class. An XNA control won't work though, so similarly to openGL, a game window will be the only solution (Whether it be implemented in openGL or XNA).

**Last meeting:** 26 April 2010

**Next meeting:** 20 July 2010

## Goals and Work targets

### Goals for this week

- discussed above

### Goals Achieved

- discussed above

### Proposed goals for next week

- Draw cube from captured packets (real time)
- Finalise Literature Review

## Rate your work performance

- How did you feel you worked ? Not enough
- Did you achieve all your goals ? No
- What were the issues you had trouble with? openGL component...
- How can you improve your performance? Stick to a rigid plan of action over the next 15 weeks
- Provide a rating out of 10 in addition to the above. 5

## Tasks/Learning

- What is the most useful/interesting thing you learned or did this past vac? calling unmanaged methods from within managed code.
- Even bad weeks usually yield something positive

## Research

- What is the most useful/interesting paper you read this week? Security Data Visualisation by Greg Conti
- List what you have been doing research wise - papers read/written/resources found
  - Network Telescopes: Technical Report David Moore, Colleen Shannon, Geoffrey M. Voelkery, Stefan Savagey
  - NIST Special Publication on Intrusion Detection Systems Rebecca Bace and Peter Mell
  - Network Intrusion Detection
  - Intrusion Detection with Snort
  - Understanding intrusion detection through visualisation
- Research should be ongoing.