Tom Atnip, Nick Crawford, Kevin Risden

CSSE477 – Webserver

We employed the following tactics:

* A load balancer that would delegate traffic to the multiple host servers
* Availability
  + Active redundancy
    - Comes with the load balancer (multiple servers)
  + Heartbeat
    - Makes note of times when the server is running, logs it to a file, and can be checked when needed
  + Timestamp
    - The server makes note of timestamps when a new socket/request is made
* Performance
  + Prioritize events
    - Used a priority queue on the requests of a socket
  + Bound execution times
    - If an HttpRequest is running too long, we kill it
  + Increase Resources
    - Comes with the load balancer (multiple servers)
  + Increase Concurrency
    - Comes with the load balancer (multiple servers)
* Security
  + Limit access
    - Users are only able to access the load balancer directly
  + Limit exposure
    - Users are only able to access the load balancer directly
  + Change default settings
    - The servers that the load balancer points to are all on different ports
  + Revoke access
    - If requests from a user are being made to frequently, they get black listed
  + Maintain audit trail
    - Implemented a logger for all actions made by/on the server

We evaluated these tactics by performing various DDOS attacks on the system with different configurations. Note that we do not think that the priority queue was effective, as the sockets did not seem to stay persistent even though we specified that they should.