CSCI 432, Group Project Part 3

Group 10

October 17, 2015

In most modern networks their is a stable, generally deterministic, data structure in place to handle requests. By definition, these deterministic systems are very predictable. Unfortunately, because of their predictability, they can be abused. Users who understand the nature of the network can overload the system with a series of time consuming requests, which eventually bog down the network. These denial-of-service (D.O.S.) attacks can occur for a variety of reasons ranging from breaching security to gaining an advantage in competitive gaming. In general, D.O.S. attacks rely on knowing how the network will respond to every request. In theory, if an adversary could not predict a network's response, then they could not mount a D.O.S. attack on the network. Knowing this, we are motivated to create a data structure that has unpredictable timing for any given input, while still performing at a near optimal speed. Such a data structure must be able to perform the same operations as the original system, while also non-deterministically, i.e. randomly, altering itself. This new system should be able to resist all timing- dependant attacks, even from attackers who know the algorithm and the previous i/o values used. In their paper, Darrell Bethea and Michael K. Reiter discuss a data structure for set operations with these desirable characteristics[1].

References

[1] Bethea, Darrell, and Michael K. Reiter, *Data Structures with Unpredictable Timing* ESORICS, 2009.