CS 1653 Phase 5

T8: DDoS Attack

Threat:

There comes the possibility that there may be an attack to the server or group servers that makes it impossible for users to actually connect. DDoS attacks are a common way to flood the ports making it hard for real users to connect to the servers.

Mechanism:

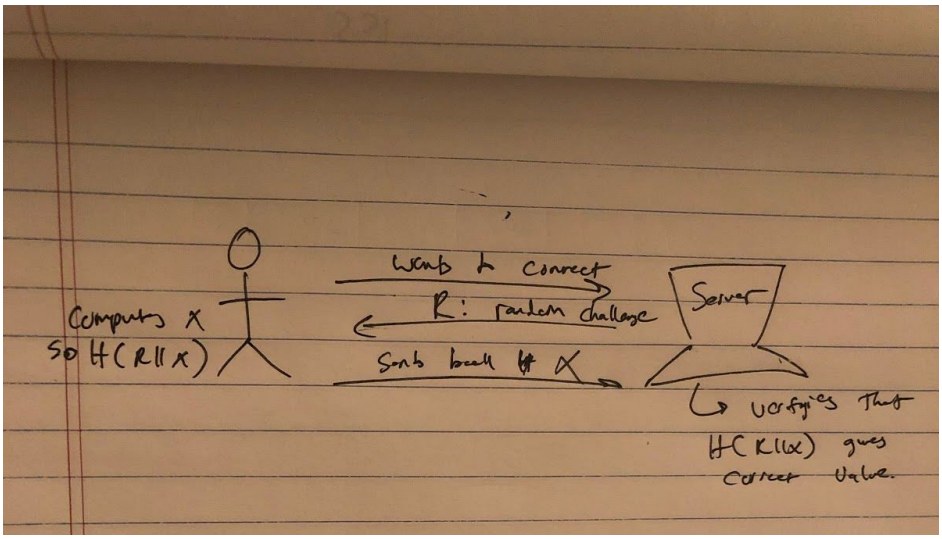

Figure 1. T8 Mechanism

The mechanism that we will use to combat this issue is a simple math problem. This acts a proof of concept as our main goal is to slow the possible connections that can link to our servers. The idea is that the server will generate two random integers that the user will have to sum up. In doing this the user will have to send back the right answer along with the two generated integers. This will hash into a valid hashmap to the server that will verify the successful hashing. Then it will grant the user the connection and ability to log into the server.

Defense:

This kind of authentication before the connection is activated gives time for the server to authenticate the connection. It will allow real users to connect instead of an active attacker that is sending out multiple requests. The level of security can be improved as in, the attacker could potentially write a program to compute the x and still launch the same attack. But the idea is that we are dealing with a naive attacker that is only using a bash script of some sort launching multiple connection attacks.