To: William H. Flathead III

From: Matteo Franzil

Subject: SYN flood explaination

Date: October 17, 2021

I am writing this memo in order to respond to the questions asked in the last few days.

To begin with, we are currently launching on our servers a simulation of what would happen if some attacker were to launch a DoS (Denial of Service) attack. More specifically, we are focusing our effort on the TCP SYN flood attacks.

A TCP SYN flood attack is a type of attack where an adversary, equipped with a hopefully powerful machine and a strong network connections, begins to bombard one or more particular machines with continuous, uninterrupted TCP connection requests. In other words, it starts sending TCP packets with the SYN flag on at a certain rate per second (usually, we talk about several thousands or millions, but for our simulations we were pretty cautious) with the intent of making the target machine unresponsive and possibly crash. This effect can be usually obtained in two ways: by cluttering the network channel, and by exhausting the target's memory. In both ways, the immediate result is that legitimate traffic, querying the server at human speed, is asphyxiated by the large amount of trash packets coming from the attacker and either never reaches the server, or if it does it may come back at a much later time - unless of course the server gives up and crashes.

While DoS attacks are particularly tricky to handle, there exist some mitigation strategies in the market that allows us at least to counter a little the work done by the attacker. One of them uses the so-called SYN cookies. AYN cookies are a mechanism, employed by the server, whose core idea revolves around using particular TCP sequence numbers, encoding the information about the timestamp, MSS and then session inside it. This has two benefits. First, it allows the server, on the receiving of the first SYN, to immediately reply and drop the memory that has been allocated for that particular connection - since, if he will receive an ACK back, he can just reconstruct the connection information from the sequence number, minus one. Secondly, it partly mitigates the risk of a DoS attack: while the network channel can and will be cluttered by the packets incoming from the attacker (and the responses from the server), the memory will be mostly unaffected and will be able to serve legitimate requests, which are correctly ACK-ed by clients and therefore deserve a space in the server memory. In other words, SYN cookies can hold off an attack as long as the memory of the server isn't the bottleneck - as the network channel will probably give up first.

The results of our research can be found in the `memo.pdf` file. There, you can find the four different scenarios that we tested, the used scripts, the results, and some graphs.