Project Report.

Reproduction of Network Research.

TCP OPT-ACK attacks.

**Original paper**

Goals

In an attempt to showcase the possibility of a network congestion from a “misbehaving” TCP client, the authors wanted to measure the impact of a singular node on a number of TCP server. In this context, the concept of “misbehaving” node is the misuse of positive acknowledgement protocol, sending an acknowledgement before the packets has been received, sending acks on the whole congestion window on each RTT ( round-trip delay) which cause a significant increase of the congestion window to the maximal point which the networking link can no longer support. This paper looks at opt-ack as a networking attack rather than the massive improvement on the end-to-end performance. The original author then goes to propose 7 different proposals that can mitigate the issue that we face with misuse use of positive acknowledgment, however they all hold different cost and benefit factor.

Motivation

The opt-ack attack were evaluated in both effectiveness and feasibility and it has shown across many different medium that I was easy to mount and I was very effective as a mode of Denial Of Service attack, allowing a possible network collapse. Though an solution was presented and it was evaluated, there is yet to be a mitigation on the implementation of the networking schema, hence in a scenario where the network is not protected in another way with potential network cap alternatives, a congestion collapse across large sections of the internet can still occur.

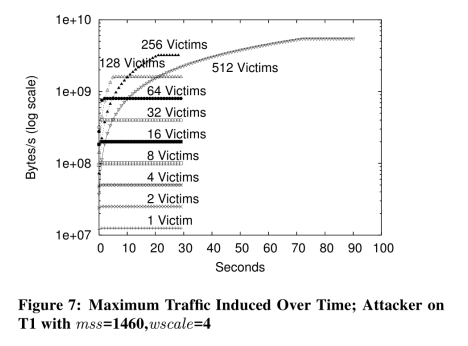
Results

The possibilities of the problem that was presented by the paper was verified. The original paper found that exploitation of the greedy opt-ack methodology has a achieved a factor of amplification that will indeed backfire to the client and network user. With a typical internet connection amplification of up to 1683 times the typical bandwidth rate and its worse condition amplification that can potentially reach 32 million times the regular rate, a regular networking link can easily be collapsed. stated, “ an attacker with a 56 kilo-bits/s modem ( beta = 7000B/s) can generate 9,351,145 B/s “ which was more than the capacity of a T3 line, which is a popular choice of internet connection for businesses that mostly depend on a reliable connection. This then was also compared to the theorical limit of a 100mb Ethernet Limitation, which was close the worst-case bandwidth amplification. The differentiation of the malicious traffic over legitimate traffic is also an issue as a it would not be locally obvious to the victim that they are participating in ab Distributed denial of service attack if they are a part of a botnet. To an external observer, like an IDS (intrusion detection system) the ack steam should in theory be indistinguishable from a completely valid high-speed connection, as it is an incoming traffic and comparatively the packet of acks is small in size.

In term of defense against Opt-Ack attack, the paper present 7 different solution in which was weighted in 4 different aspect, Efficient, Robust, Deployable, Simple. With this, the paper found that randomly skipping segment at the server shows most promise. Based on the considerable experimentation, the solution was able to hold over 99% efficiently while preventing the attack. This was also with one minor fix on the random selection, with possible optimization schema, it can solve the problem with only 0.01% error rate.

Reproduction Work

Motivation and Goals

The goal of this project is to go through the experimentation and replicate the attack that was presented in the paper. Our main motivation is to recreate the high bandwidth utilization at the victim server caused by a client low bandwidth connection. This was presented in the figure 7 diagram in the original paper, which shows just how much traffic an attacker that is connected to multiple servers can emit when maliciously utilize the optimistic Acknowledgement attack. The result diagram caught our eyes as it proves the effectiveness and possibility of such attack to occur.

Challenges

Result

Platform