SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks

Summary : In this paper, a novel defense mechanism is presented called SIFF (Stateless Internet Flow Filter) to prevent the DDoS or DoS attacks. It allows an end-host to selectively stop individual flows from reaching its network, without keeping per-flow state in the network. This paper also explores the design issues involved in constructing a system from scratch that solves the DDoS flooding problem by giving a packet receiver control over which packets the network delivers to it. SIFF enables the victim of a flooding attack to stop individual flows from reaching it before the flows saturate its network. In SIFF, network traffic is divided into two classes, privileged (prioritized packets subject to recipient control) and unprivileged (legacy traffic). The view from ten thousand feet is as follows - clients and servers participate in a handshake using a specific type of unprivileged packet known as an EXPLORER (or EXP) packet. Routers insert path specific information into EXP packets, who's aggregate among all the routers in the path is used as a capability token for a privileged channel between the client and the server. After the handshake, clients and servers communicate using privileged packets called DATA (or DTA) packets, into which they insert the capabilities carried in the EXP packets. When routers forward a DTA packet, they first check to see if part of its capability equals that information which would have been inserted into the packet had it been an EXP packet. If the markings match, then the packet is forwarded. If not, then the packet is immediately dropped. One important assumption made here is that the IP headers has sufficient space to accommodate the information that routers mark in the packet. Also, if the router information inserted into packets is static then an attacker could simply obtain the capability through a seemingly legitimate request. To prevent this, router key switching mechanism is introduced.

Opinion : This paper talks a lot about different ways of sneaking information from the system and at the same time, it also provides solutions for the same. For example, the key switching mechanism provides a good way of hiding router information and the probability of guessing is given by $P(x, z) = 1 - (1 - 1/(2^z))^x$, where x is number of marking each router maintains and z is bits per router marking. Also, the hash function for calculating the marking can be improved. The marking is calculated as the last z bits of the output of a keyed hash function with the following parameters as input: the IP address of the interface at which the packet arrived at the current router, the last-hop router's outgoing interface IP address 3, and the source and destination IP addresses of the packet being forwarded. Here an adversary can guess the last z bits of the hashed value.

Pros and Cons : Let's talk about the pros first. To start with, the use of source IP address as an input for the hash function prevents spoofing of source IP address. Secondly, Routers need not maintain a large set of information. No ISP cooperation is required. Lastly, little per packet processing is required at routers. Now for the cons, the first big assumption is that the victim has the ability to determine that it is under attack. The second big assumption is that all router can implement SIFF which might not be the case. Lastly, the processing at each router will add some latency which is undesirable.

Thanks