Detecting Prefix Hijacking Through Active and Passive Measurements

The Internet is a distributed collection of networks with no central authority. Such a system lends itself to the tremendous growth we see today. However, the Internet's distributed nature is prone to many security flaws. Prefix Hijacking is one such flaw in which a network steals address space from another network effectively diverting the victim network's traffic. Such an attack can be used to effectively deny inbound traffic and can also render large portions of the Internet unavailable depending on the scale of the attack. Many of these events have been recorded with some targeting specific sites such as YouTube while others have hijacked vast portions of the allocated address space. In our work we have developed tools and strategies for detecting Prefix Hijacking in real time. By using both passive triggering from real time BGP updates and active probing tools such as traceroute and the ping utility we can catch origin network changes for prefixes and verify whether the traffic to those address blocks is still reachable. With such a tool a network operator can be notified immediately of a prefix hijacking. Since such an event is rare our initial experiments have been to prove our work as a proof of concept and show that such measurements are possible and accurate.