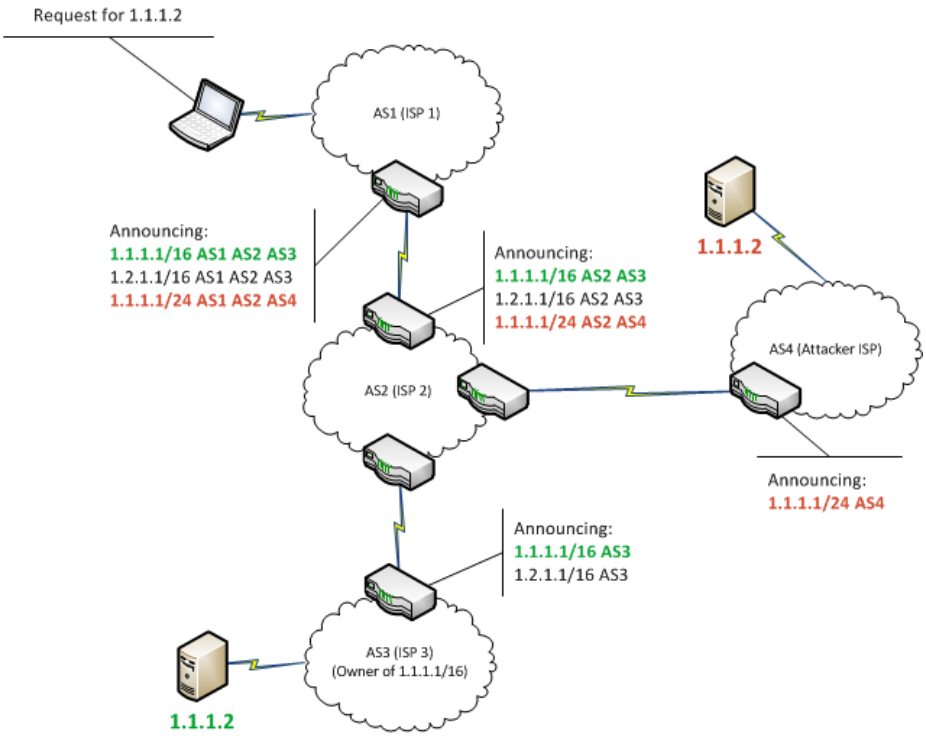
BGP Prefix Hijacking Attack Investigation

Abstract:

The Internet infrastructure was not designed with security in mind, and is consequently alarmingly vulnerable. It is based on Border Gateway Protocol (BGP) which performs the routing between administrative domains, or "Autonomous Systems" (ASes) , and is considered as an insecure protocol.

One of the known attack on BGP is BGP hijacking. Cybercriminals and governments alike have taken advantage of this technique for their own ends, such as traffic misdirection and interception. The hijacking is based on the fact that BGP determines how data flows from its source to its destination. By manipulating BGP, data can be rerouted according to the attacker's choise, allowing them to intercept or modify traffic. Internet-level BGP hijacking is performed by configuring an edge router to announce prefixes that have not been assigned to it. If the malicious announcement is more specific than the legitimate one, or claims to offer a shorter path, the traffic may be directed to the attacker. Attackers will frequently target unused prefixes for hijacking to avoid attention from the legitimate owner. By broadcasting false prefix announcements, the compromised router may poison the Routing Information Base (RIB) of its peers, as shown below. After poisoning one peer, the malicious routing information could propagate to other peers, to other Autonomous Systems, and onto the broader Internet.



Goals:

a. Use Cisco VIRL and create 3 different internet topologies that 5 or more ASes. Use https://www.youtube.com/watch?v=6p4xudEvCrI as reference.
b. Simulate BGP Hijacking interception (man-in-the-middle) attack and “black-hole” attack on each of topologies using Routem anf traffic generator on VIRL.
c. Compare between the topologies and the attacker placement and suggest when the attack is more common to succeed.

Requirements:

Internet Networking Course