A Configuration based Approach to Mitigating Man-in-the-Middle Attacks in Enterprise Cloud IaaS Networks running BGP

Abstract

Cloud IaaS service providers offer virtualized computing resources to enterprises over the internet. As with most internet based services, cloud service providers may need to establish BGP peering relationships with upstream/neighbor ISPs for the purposes of exchanging routing information between their respective Autonomous systems thereby making it possible for a rogue AS to carry out a Man-In-The-Middle (MITM) attack. Available literature supports the fact that BGP as an infrastructure protocol is vulnerable to MITM attacks yet a good number of proposals aimed at counteracting these attacks have not been fully implemented. Secure BGP, Secure Origin BGP and Pretty Secure BGP are all proposals which have not been fully implemented due to high overhead and invariable router load. We believe however that an existing cloud IaaS service provider could mitigate the risk of a MITM attack by optimizing their configurations and ensuring that upstream providers do a proper job filtering prefixes using a prefix-list. This paper presents a GNS-3 simulation of a MITM attack by mimicking a section of the internet and goes on to show how the application of a prefix-list can help mitigate the attack.
A Configuration based Approach to Mitigating Man-in-the-Middle Attacks in Enterprise Cloud IaaS Networks running BGP

References


Index Terms

Computer Science Information Sciences

Keywords

BGP security, Cloud Services, Prefix-List, Secure BGP, Session Hijacking.