Losing Control of the Internet:
Control Plane Attacks via the Data Plane

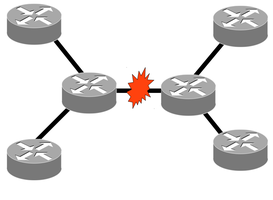
Max Schuchard, Abedelaziz Mohaisen, Eugene Y. Vasserman, Denis Foo Kune, Yongdae Kim, Nicholas Hopper
University of Minnesota

Introduction

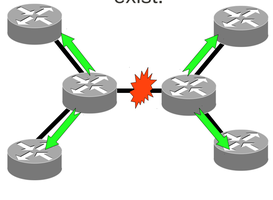
The Internet was designed to be robust to local failure and to adjust to route around outages. However, Internet control plane events propagate globally; as a result, an excess of these events can disrupt core Internet routers. This disruption can lead to network instability, resulting in loss of connectivity and data. We investigate the possibility of intentionally and repeatedly generating these incidents without compromising BGP speakers. These attacks can be carried out in a targeted and repeatable manner causing disruption to the core Internet routers, taking large portions of the Internet offline.

BGP's Global Nature

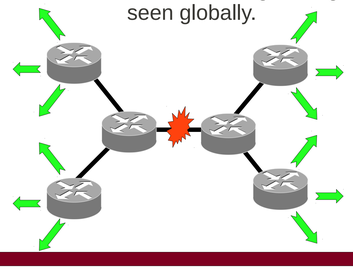
A local network change results in the failure of a BGP session between two routers. They now must withdraw routes discovered via each other.



BGP update messages are sent from the affected routers to their peers, notifying the peers that a collections of routers no longer exist.



The BGP peers will then possibly send BGP updates to their peers, who may do the same. This can result in the local change being seen globally.



Attacker Generated Local Events

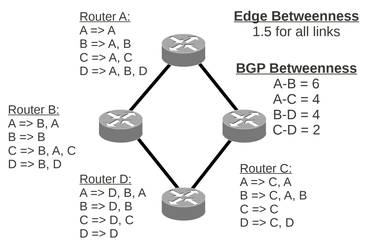
- Zhang *et. al.* Provided the attack to do this [CITE ME]
- Attacker uses data plane traffic to disconnect routers
- Possible because control plane and data plane are co-located
- When resources are scarce both data packets and control packets are dropped
- Enough dropped control packets cause routers to disconnect from each other

The CXPST Attack

· The Coordinated Cross Plane Session Termination Attack
· Applies Zhang *et. al.*'s attack in a targeted manner
· Adversary uses botnet to select key BGP sessions to disrupt
· The goal is to maximize the number and scope of the resulting BGP updates
· By generating large numbers of updates CXPST overwhelms the computational capacity of routers

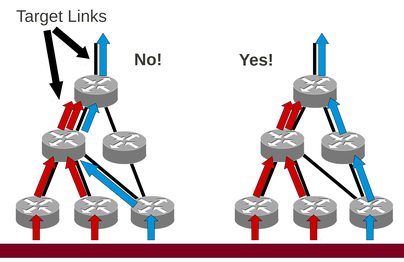
Target Link Selection

•Edge betweenness fails as BGP does not always use the shortest path
•Betweenness based off of BGP paths provides a superior selection metric



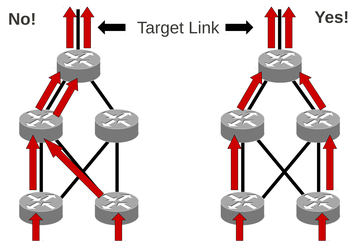
Attack Path Independence

•Attack traffic needs to not travel more then one targeted link
•Prevents changing topology from deflecting attack traffic

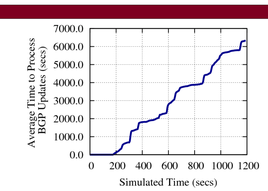


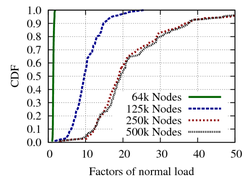
Attack Path Diversity

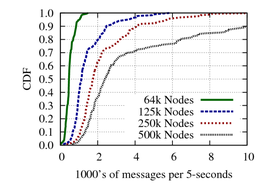
•Attack traffic needs to be spread across multiple links in transit to target
•Reduces chance of accidental topology changes



CXPSTN Simulation Results



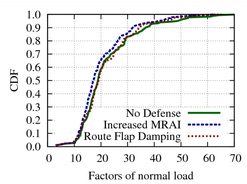


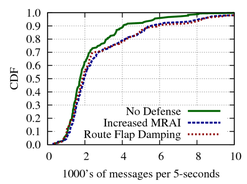


Defenses Against CXPST

- CXPST is closely related to route flapping
- Route flapping defenses exist and might be useful
- Minimum Route Advertisement Interval increases prevent rapid re-advertisements of networks
- BGP Graceful Restart delays when routes are withdrawn after two routers disconnect
- Route Flap Damping tries to limit re-advertisements in the long term
- None of these defenses work against an intelligent adversary

Beating Existing Defenses





Stopping Session Termination

- Instead of controlling the scope of updates, stop Zhang *et. al.*'s attack
- Can be done by stopping BGP from automatically disconnecting during control plane packet loss
- Works when partially deployed to largest ASes