Demo: BGP Path Hijacking

Vimal

Stanford University

August 18th 2014
Goals of the Assignment

• Understand how BGP path hijacking attacks might happen in the real world.

• Give students a hands-on experience, and a platform to explore beyond the primary goal.
Outline

• Why is Mininet helpful?
• Assignment walk through
• Behind the scenes
Why is Mininet helpful?

• Easy to setup the environment
  – No need for expensive routers or VMs.
  – No need to simulate BGP protocol. Use production-quality software!
  – Explore various parameter tweaks readily.

• Easy to access state information
  – cat /path/to/logfiles
  – tcpdump

• Easy to distribute the assignment
  – git clone ssh://git@bitbucket.org/jvimal/bgp.git
Assignment Walk Through

• Step 1: Set up the environment on Mininet
Assignment Walk Through

• Step 2: Start R1, R2, R3. Log into R1’s routing daemon.
Assignment Walk Through

• Step 3: Peek into R1’s routing entries.

• Step 4: Start browsing a 13.0.0.0/8 website at AS1 in a loop.
Assignment Walk Through

• Step 5: Start the rogue AS.
  – Wait for convergence.
  – Watch what happens to website browsing loop.
  – Check the routing information base in R1.

• Step 6: Stop the rogue AS.
Behind the Scenes: Network Namespace (Isolation)

Container: Encapsulates the processes into its own network namespace.

August 18, 2014
Behind the Scenes: Quagga Routing Suite

• Configure static IP addresses for AS1, AS2, etc. and set up static routing entries.
• Configure bgpd’s peers inside each AS.
• Set up zebra to program Linux Kernel’s routing entries (no need for OpenVSwitch).
Things to try out

• Try tcpdump on BGPv4 messages
• Try larger topologies and plot BGP convergence times
• Replay BGP updates in Internet (RIPE data) and the entire Internet2 (dataset available online)
• Try other kinds of attacks (announcing more specific prefix with a larger path)