

# Stealthy IP Prefix Hijacking

Don't Bite Off More Than You Can Chew

Authors: Christian McArthur  
Mina S. Guirguis

Texas State University-San Marcos

# Border Gateway Protocol

- Internet is composed of multiple Autonomous Systems (ASes) or networks (ie Texas State, Microsoft, AOL, Level 3).
- Border Gateway Protocol (BGP) used to determine how packets traverse the ASes.
- ASes announce to providers IP prefixes it originates. Announcements are propagated through Internet.
- BGP vulnerable due to its trusting nature.

# Prefix Hijacking

- Attacker falsely announces that it originates a prefix (or subprefix).
- Or attacker falsely announces that it lies on the route to the prefix.
- Existing research almost entirely focuses on large scale attacks.

# Non-Large Scale Attack

Goal: Hijack a prefix such that I attract a small amount of traffic.

“Benefits:”

1. I can easily manage the traffic (bandwidth limitations, processing).
2. The victim may not notice a smaller decrease in traffic.

Additional Goal: Evade detection.

# Stealthy Prefix Hijacks

- Attacker announces a path to the victim short enough to attract some traffic, but long enough its effects are not wide scale.
- “Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew,” Christian McArthur and Mina S. Guirguis, SIGCOMM 2008, Poster

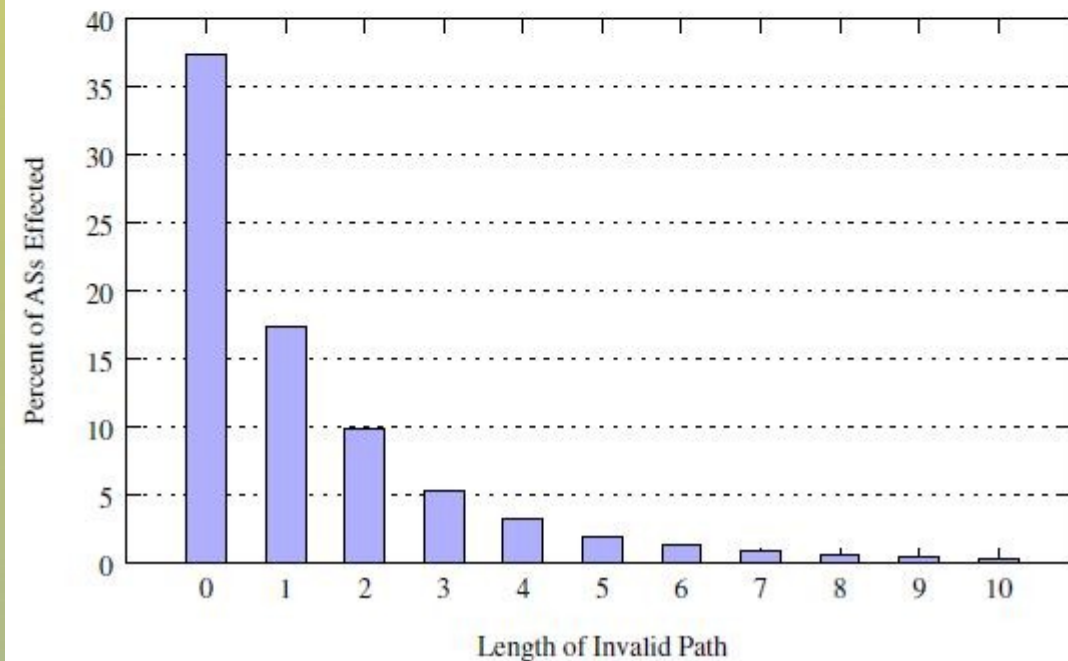
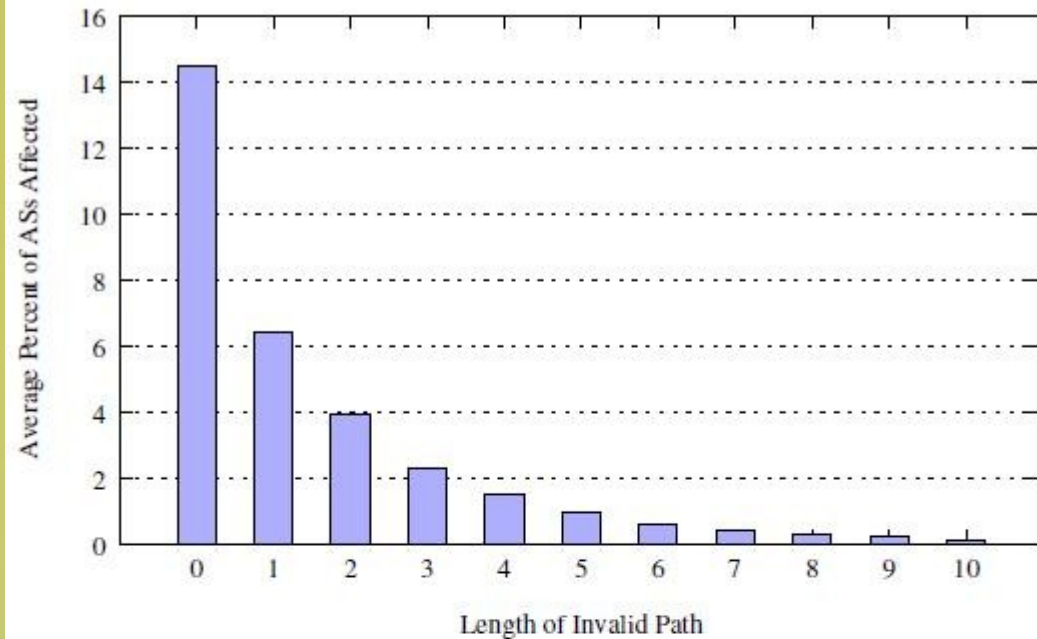
# Effects of a Stealthy Hijack

- BGP routing data provided by Routeviews.org on March 4, 2008.
- For each of 250,000 prefixes in this data, the AS trees (routing paths) were reconstructed.
- Each AS in the tree was evaluated to determine if traffic from the AS to the victim could be hijacked with hijacked paths of length 0 to 10.

# Effects of a Stealthy Hijack

- As length of path increases, fewer percentage of ASes are effected.

- Top: Average ASes effected
- Bottom: Maximal ASes effected



# Initiating Hijacks

- 1) Discover the AS tree for your chosen victim.
- 2) Determine which ASes in the tree you can be a customer of.
- 3) For each provider, estimate the potential effects of the hijacking with differing lengths.
- 4) Establish a relationship with the provider.
- 5) Announce an invalid BGP route for the victim and analyze the amount of incoming traffic.
- 6) If the amount of traffic is not desired, repeat 5) with a BGP announcement with a different length. If there is too much incoming traffic, make the length longer. Otherwise, make length shorter.

# Detecting Prefix Hijacks

- Prefix Hijack Alert System (PHAS)
- Hop Count Changes in IP Traceroute
- Traceroute Path Disagreement
- AS Traceroute/BGP Route Comparison
- Heuristic Examination of BGP Updates
- iSPY

# Detecting Stealthy Prefix Hijacks

- No one detection mechanism seems to be able to detect stealthy hijacks.
- Proposal: Combine two ineffective detection methods to become effective.
  - 1) Comparison between AS Traceroute & BGP routing announcements.
  - 2) Comparison of traceroutes between the target/victim and a reference point.

# Detection Overview/Algorithm

- 1) Perform IP traceroute to possible victim.
- 2) For each router in the traceroute, convert IP address to AS number.
- 3) Compare AS traceroute to BGP route.
- 4) Perform AS traceroute to reference point.
- 5) Compare AS traceroutes of target & reference point.

# Conclusion

- We examined a method of prefix hijacking largely unresearched.
- Discovered it is possible to perform a stealthy prefix hijacking with a high degree of granularity.
- Examined the potential effects of stealthy prefix hijacking.
- Devised a way to effectively detect hijacking attempts.