BGP Attack Trees: Real World Examples

Sue Hares, NextHop

BGP attacks - Why Should we talk about them?

Sue Hares, NextHop

Homeland Security on Secure Infrastructure

- Attack on Root Servers In October ’02 caused:
  - "***We're looking at institutionalizing the standard protocols for communication back and forth" between the root-server community and the U.S. government,*** Schmidt said in comments to Technology Daily following his speech to the SecurE-Biz conference in Arlington, Va.” 4/1/03
- “National Strategy to Secure Cyberspace” (2/17/03)
  - Strategy to Secure Cyberspace," ***whose goal is to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."***
  - Includes: intrusion detection, Internet infrastructure security (including protocols such as BGP and DNS)
  - 1-5 year plan

Panel to Call for Presentations and Pub Session

- Panel's start
  - At IETF in March, Vijay Gill provided "things" we could do to help his BGP peers security
  - BGP is ready to replace 1771 with new draft. Security issues are key.

  Operators look at BGP deployed

- Call for presentations at NANOG 29

Public discussion difficult

"It is a disservice to the community to talk about the existence of exposures without being specific about what those exposures are.

There is always the "only tell the good guys" factor but that only goes so far. In reality you have to "tell the good guys first".

Curtis Villamizar

Query to Reality of BGP attacks

- Erik Shrek, MCI
  - “To be honest we have never seen any real attacks directed at BGP. There seem to be a lot of people focused on this, but the attacks are relatively hard to do compared to a ton of other attacks that are much easier to do.”
- Bill Norton
  - "We are not aware of any attacks on co-located BGP infrastructure."
- Vijay’s comments on BGP problems
  - RPF checks, local network checks
  - Network Filters: prefix, network bogons, TCP MD5

Attacks and Fixes

- High amounts of prefixes flooding
  - Normal reason: mis-configuration
  - Fix: maximum prefix filter, prefix filters
- SYN Floods to port 179
  - Reason: Attack
  - Resolution: TCP MD5, limit access to TCP port via filtering
- Internal multi-hop BGP session high-jacked, route injection of bad blocks causes network failure
  - Reason: clear text passwords, session available to high-jacker
  - A Solution: multi-hop BGP over IP-Sec tunnel

Enterprise comments

Mike Lloyd, RouteScience

- Ask an enterprise its reaction to “BGP Attack Trees”
- Majority response: “Huh?”
- An Opinion on what we could change
  - Strong Routing Registry infrastructure helps

Attacks go after Infrastructure

- Deployed boxes at sites
- BGP Vulnerabilities (see earlier talk)
  - TCP, MD5, BGP errors
- Deployment issues (BCPs)
  - RPF checks, local network checks
  - Network Filters: prefix, network bogons, TCP MD5
  - AS Path Filters
  - Blind attackers
- Configuration of Routers or Firewalls
  - Methods of router configuration distribution
  - Registries (private and public) Private registries
  - Origin Security (INV, S-o-BGP)

90% Mis-configuration: Is it out of synch or inconsistent policy due error, accident or a attack?

Beer Discussion – Macro Discussion

- How do we keep the Federal Government “clue-ful” about BGP Infrastructure costs?
- What will minimize the costs of a BGP infrastructure outage?
- Any other reports you’d like to whisper to me about?

Other Reports of BGP attacks

Steve Bellovin, AT&T research