# BGP Security, Availability, and Operator Needs

David Meyer/Andrew Partan
dmm@1-4-5.net/asp@partan.com

NANOG 28
Salt Lake City, Utah

# Agenda

□ What problem(s) are we trying to solve?

□ So why are/aren’t we deploying a "secure" BGP?

□ Complexity Issues?

□ So what is the 10K-mile goal anyway?

□ Discussion

□ http://www.1-4-5.net/~dmm/NANOG28/s-o-bgp

# What problem(s) are we trying to solve?

- Lots of threat model work, including
- Configuration mistakes
- Prefix hijacking
- Compromised backbone routers
- Availability
- New attacks?
  - "Using Link Cuts to Attack Routing" [Bellovin,Gansner]
- And all of those things we haven’t seen/detected yet...

# And in case you were wondering...

"I would stress that all of these things, particularly prefix hijacking and backbone router ’ownage’, are real threats, happening today, happening with alarming frequency.  Folks need to realize that the underground is abusing this stuff today, and has been for quite some time."

-- Rob Thomas

# So why aren’t we deploying a "secure" BGP?

- Note that there are two works-in-progress
  - sBGP and soBGP
- So why aren’t either of these being deployed?
- Community consensus
- Complexity
  - But there is a paradox/tradeoff here
- "Complexity is the enemy of security" -- smb

# Complexity...

- Both sBGP and soBGP seek to protect different parts of the routing system via cryptographic means
  - allocation of IP addresses/AS numbers
  - granting routing authority for a chunk of address space
  - and for of the BGP messages and peerings
    - note that soBGP doesn’t envision protecting the session/peerings as the authors see that as a different part of the overall problem.
- That is, you (might) want to authenticate every step of the allocation of an IP address
  - from IANA to the Registries
  - to an ISP to another ISP to a customer
  - to AS number allocations
  - to permitting an AS to originate routes to some address space
  - to all BGP traffic - AS paths and next hops, etc

# Pragmatism and the complexity challenge

"My trepidations regarding complex tasks is based on our experience with simple tasks.  How many BGP speaking routers don’t have VTY ACLs?  Too many!  We can’t even get "simple" deployed, so what chance does "complex" really have?  I’m not trying to be a pessimist, but I am trying to be pragmatic."

-- Rob Thomas

# So what is the 10K-mile goal?

- (Almost) every BGP speaker should be able to verify:
  - that the address space has been properly allocated
  - that the origin AS is valid
  - that the entire AS path is valid
  - and what about other attributes (e.g. VPN?)
    - and BTW, are there security/other implications of (continuing to) throw (almost) everything into BGP?
- Note that there are cryptographic signatures that will need to be checked and verified at each step
- So at 10K, this is probably what you would like
- But all of this comes at a price:
  - Additional operational complexity and infrastructure

# So what can or should we do?

- How about....
  - Pre-collecting all of the published information into one local database and running authorization checks there
  - Only send a router this ’precompiled’ chunk of data instead of everything
  - But the router still need additional processing and memory to be able to handle this
- Still: Its unclear how big this precompiled information would be, or how much of it a router will need when it restarts
  - How much do you need to cache on the router itself?
  - You may no longer have a routing system that can come up by itself

# So what can or should we do?

- Finally, there is a non-trivial amount of infrastructure needed for all of this
- Databases and certificate authorities and all of the rest
- And what is the effect on BGP convergence properties?
- And who pays?
  - CAPEX/OPEX is the frontier for the carriers these days
  - And what about "free market" issues?
    - What stops users from moving to lower-cost ISPs who do not implement this?
    - New kind of "No-SLA" service?

# How about administrative delay for soBGP?

- In soBGP, the signatures and cerificates have to be generated the same way as sBGP

- However, the propagation of this information is significantly different.

  - Instead of relying on out-of-band databases (and their syncronization), the certificates are advertised in a new Security Message.
  - This means that once a new block is allocated (and the certificates created), the security information can be propagated to everyone in the system at about the same rate as UPDATE propagation.

- So in theory, soBGP won’t add admistrative delay

# How about administrative delay for sBGP?

- So will it take longer to get a new address block routed under sBGP?
- Maybe
- Why?
  - Hypothesis: All of the various signatures involved will first have to be generated, signed and published to a local database,then pushed to some global database(s), and then copied to each ISP’s own local databases, checked and recompiled, and propagated to each router...
- So, are we willing to wait?

# And (sort of) finally....

- If you think about the additional processing and memory and storage needed on a router, there are a fair number of routers that are adequate for today's needs but will be out of their depth with the new requirements.  A lot of upgrades and replacements would be needed...

- And again, who pays?

# Alternate Position

- How much of the problem can be solved by currently deployed techniques including BTSH, ingress filtering, unicast-RPF, and the current registry system/language
    - RFC 2827/BCP 38  ingress filtering
    - draft-gill-btsh-02.txt BTSH
    - RFC 2622   RPSL
- Would this be enough?
- And how would you define "enough"?
- And for how long?

# A few final thoughts

- What are the cost/benefit tradeoffs are we looking at?
- And is there an incremental deployment approach?
- For example, can we start with signed-origin sBGP so the machinery is present for signed-AS_PATH in the future?
- Note that soBGP doesn’t sign UPDATES
  - Certificates are advertised in the new Security Message.
- Oh yeah, and convolve all of this with IPv6....

# Questions/Comments?

- Reading
  - soBGP: ftp://ftp-eng.cisco.com/sobgp/index.html
  - sBGP: http://www.net-tech.bbn.com/sbgp/sbgp-index.html
- Next Steps?
- Thanks