BGP Security

Eric Osterweil
Primitives: how do we “secure” inter-domain routing (BGP)?

• BGP uses resources and adjacencies to create topology
  – Participants assert reachability for ASNs and IP prefixes and “gossip” about what they’ve heard from each other

• We’ve lacked a rigorous way to automatically learn:
  – Who is the rightful holder of a resource?
  – Who is allowed to assert reachability for resources?
• Also, who is authorized to “gossip” to whom (and about what)

• Are these “threats?”
Titleship: who is allowed to hold what

• The community has been looking at numbered resource certification (RPKI)

• RPKI is a hierarchical verification model (note ``PKI'' in the name)

• IP addresses are also allocated hierarchically
• IP addresses are allocated hierarchically
  – So, represent that w/ crypto objects

• RPKI envisions an IANA trust anchor that delegates resource allocations to RIRs
  – RIRs then sign objects for *their* allocations
  – But... We don’t have a global root today, so we have added complexity

• So... A prefix may have been allocated from IANA to ARIN to Level(3) to a customer...

http://rpkispider.verisignlabs.com/
But...

• Announcements and routing policy are authorized by resource holders *bilaterally*
  – Peering arrangements are not hierarchical

• Routes are computed by applying policy on a hop-by-hop basis
  – Validating origins maps cleanly to allocation titleship, but does not map cleanly to verifying routes

• Are there any threats that are posed along the data path of routing?
Gap analysis

• RPKI (and any derived authentication) verifies origins
• Without verifying policy bilaterally, attacks along the data path become difficult to address
• Issues like route leaks (which happen after origins) are bilateral policy violations
  – These issues can result in Man-in-the-Middle attacks [1]

Forward

• Are attacks on the data path not important?

• Do we need additional thinking?

• Should we revisit our conception of threats?
Thank you

Questions?