Why don’t we have a Secure and Trusted Inter-Domain Routing System?

Geoff Huston, APNIC

Why do we keep seeing these headlines?

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

THE ACCIDENTAL LEAK —

Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

DAN GOODIN - 11/13/2018, 6:25 PM

Google lost control of several million of its IP addresses for more than an hour on Monday in an event that intermittently made its search and other services unavailable to many users and also caused problems for Spotify and other Google cloud customers. While Google said it had no reason to believe the mishap was a malicious hijacking attempt, the leak appeared suspicious to many, in part because it misdirected traffic to China Telecom, the Chinese government-owned provider that was recently caught improperly routing traffic belonging to a raft of Western carriers though mainland China.

FURTHER READING
Strange snafu misroutes domestic US Internet traffic through China Telecom

The leak started at 21:13 UTC when MainOne Cable Company, a small ISP in Lagos, Nigeria, suddenly updated tables in the Internet's global routing system to improperly declare that its autonomous system 37282 was the proper path to reach 212 IP prefixes belonging to Google. Within minutes, China Telecom improperly accepted the route and announced it worldwide. The move by China Telecom, aka AS4809, in turn caused Russia-based Transtelecom, aka AS20485, and other large service providers to also follow the route.

According to BGPmon on Twitter, the redirections came in five distinct waves over a 74-minute period. The redirected IP ranges transmitted some of Google's most sensitive communications, including the company's corporate WAN infrastructure and the Google VPN. This graphic from regional Internet registry RIPE NCC shows how the domino effect played out over a two-hour span. The image below shows an abbreviated version of those events.

1. The Meta Goal

Can we devise changes to operational practices, or operational tools or routing technologies that manage the inter-domain routing system that could prevent the propagation of false or artificial routing information in the Internet?

This is a Very Challenging Goal

- It’s a problem as old as the concept of a distributed inter-domain routing system
- Each actor applies local policy constraints on local topology knowledge to guide its local route object propagation decisions
- No single actor has sufficient “whole of system” data to determine the difference between what it should’ve learned and what it has learned

The ideal

We want the interdomain routing system to advertise the **correct** reachability information for “**legitimately connected”** prefixes at all times

That means that we want to **avoid**:

- promulgating reachability for bogus address prefixes
- promulgating incorrect paths for reachable prefixes
- blocking paths for legitimately connected prefixes

The problem

While we'd like to think we understand the provenance for each and every IP address, that is not exactly the case

And even if we did, we have no precise knowledge as to which network has the authority to originate a route object for that address

And even then we have no exact knowledge of the inter-domain topology of the network

And even then we have no clear knowledge of the local policy constraints that are applied to the propagation of reachability and topology information

The problem

All of which means that we have no clear model of “truth” to compare to the information flow in the routing system

1. A Weaker Goal

Can we devise changes to operational practices, or operational tools or routing technologies that manage the inter-domain routing system that could resist attempts to inject false or artificial routing information in the Internet?

2. What Data would we like?

- An (impossible) ideal data set is the “reference set” that describes a ‘correct’ route object set that should be visible at any vantage point in the network
  - And access to a set of credentials that support any such attestation of “correctness”
- As a compromise we could settle for a reference set that describes a ‘stable’ route object set that should be visible at any vantage point in the network

What we want and don’t want

- BGP anomaly detectors and observatories are all well and good, but they have not proved to be all that useful to the operations community
  - They are a bit like smoke alarms – they can’t prevent the root cause, but simply alarm after it happens
- **What we would like is some form of route acceptance model that can be used as an acceptance filter**

Some 10 years ago…

- We observed that we needed to improve “truth” in addressing and routing
  - We designed a PKI to allow digitally signed attestations about addresses and AS numbers for use in routing
  - We published tools to allow network operators to use this PKI
  - We supported security extensions to BGP to make use of these signed attestations - BGPSEC

Is BGPSEC the Answer?

- Yes and No
  - Yes, it can reject anomalous BGP updates upon receipt of the update
  - But:
    - it relies of the correct operation of the protocol, not the correct implementation of policy
    - It is very expensive to run
    - It relies on comprehensive adoption, and partial adoption is a worst case scenario for this protocol

What's going wrong?

- BGP hijacking is not perceived as something we should work hard to prevent
  - BGP hijacking is not an end in itself, but a part of a larger attack
    - E.g. April '18 MyEtherWallet raid was an attack involving a domain name registrar, the DNS, a susceptible certificate authority and a BGP route injection to work
- The economics of this situation work against it
  - Apparently there are inadequate commercial drivers to undertake extensive informed route monitoring that would enable hijack suppression at source
  - Probably because integrity of common infrastructure is everyone's problem which in turn quickly becomes nobody's problem

How should we look at routing insecurity?

- Is this a failure of technology?
  - If we had a better routing widget then we would no longer have a problem
- Is this an instance of failure in the market?
  - Providers see no marginal competitive advantage in deploying these tools
- Is this a regulatory failure?
  - If we have to turn to some form of imposition on network providers to secure the routing system then how will we do this?

    (The current national and regional regulatory examples in content control and encryption are woeful examples! Whjy would comparable efforts in routing security fare any better?)

What should we do?

- “Let’s do nothing” is an unsatisfactory response
- But anything other than “nothing” seems to head towards pointlessly ineffectual!