

A look at the operator community's
understanding of and response to
the route hijacking threat.

Joel Jaeggli
joel.jaeggli@nokia.com

Blast from the past

A Routing Filtering Model for Improving Global Routing Robustness - an IOPS proposal

Jessica Yu

ANS Communication Inc.

Feb. 9th, 1998

What's the Problem?

- Dec 97 was AS 7007 leakage


- ◆ Current global routing system is open thus vulnerable
- ◆ 'Bad' routing information injecting from anywhere of the Internet will be propagated allover resulting outages (one dead mouse spoils the whole pot of soup)
- ◆ Proven by several incidents occurred - unfortunately

The present day

- Well, we haven't exactly been complacent since 1997 have we?
- Or maybe we have...
 - Youtube?
 - Con-ed (2006)

Hijacking Frequency

- Bush, Boothe, and Hiebert 2006 – Between 26-95 successful prefix hijackings a month (Dec 05)
- Since then a number of tools have been developed to try and get a handle on the events

PHAS  | PHAS: Prefix Hijack Alert System

Period: 2008.12.21 16:00:00 to 2008.12.22 15:59:59 (UTC)

Total Alarms: 13346
Total prefixes involving alarms: 9555
Total prefixes observed till 2008.12.22 15:59:59 (UTC): 301303

Origin

Alarms: 436
Prefixes involving alarms: 307
Prefix with most alarms: 218.99.8.0/21 with 5 alarm(s)
Alarm frequency for each prefix:

Alarms	1	2	3	4	5~10	11~20	21~30	>30
Prefixes	201	90	11	3	2	0	0	0

LastHop

Alarms: 11733
Prefixes involving alarms: 9357
Prefix with most alarms: 63.218.120.0/23 with 25 alarm(s)
Alarm frequency for each prefix:

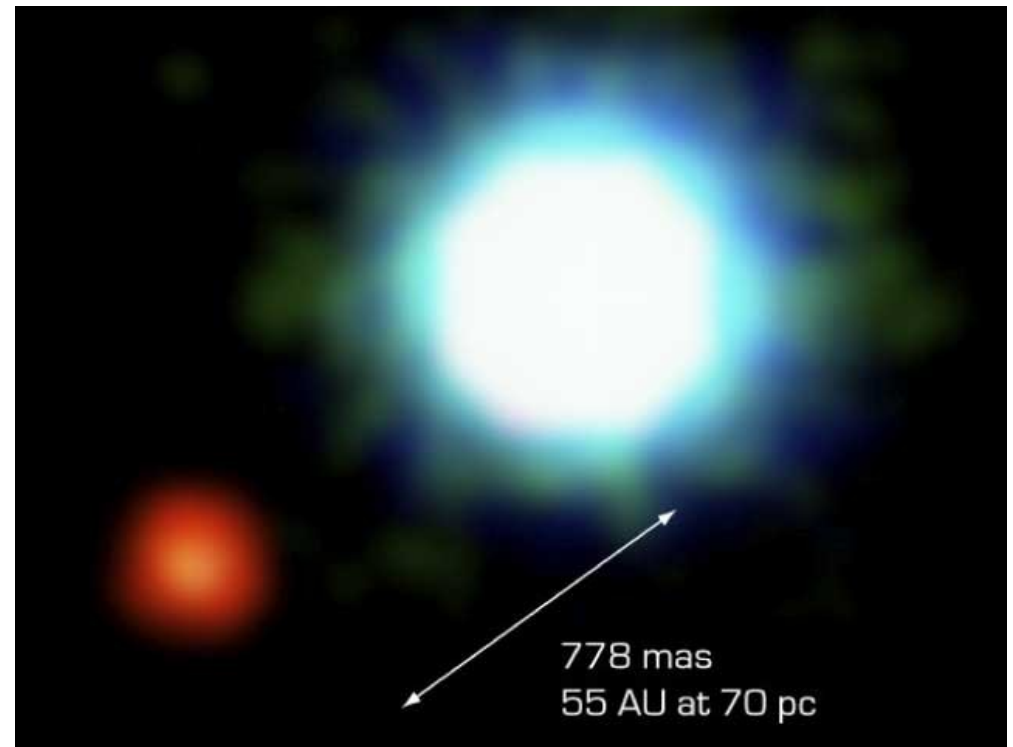
Alarms	1	2	3	4	5~10	11~20	21~30	>30
Prefixes	7710	1224	253	115	51	3	1	0

SubAllocation

Alarms: 1177
Prefixes involving alarms: 400
Prefix with most alarms: 78.129.0.0/17 with 66 alarm(s)
Alarm frequency for each prefix:

The Problem with looking for events...

- Is that the more you look.
- The more you eventually see.



Malicious, Accidental hijack or simply anomalous activity

The screenshot shows the Thunderbird email client interface. The window title is "Inbox for joelja@bogus.com - Thunderbird". The menu bar includes File, Edit, View, Go, Message, OpenPGP, Tools, and Help. The toolbar contains icons for Get Mail, Write, Address Book, Decrypt, Reply, Reply All, Forward, Delete, Junk, Print, and Stop. The search bar on the right contains the text "174.128.31.0/24".

The left sidebar shows the folder structure for "joelja@bogus.com" and "Local Folders". The "joelja@bogus.com" folders include: Inbox (396), Drafts (38), Sent (2), Trash, Deleted Messages, duplicates, fedora, freerad...13223, imapidx, Junk (2957), Junk E-mail, linux-k...(46556), routeviews (121), saved-messages, Sent Messages, spam, and squid. The "Local Folders" include: Unsent, Drafts, Sent, Trash, nanog (100), opsec (1), and rancid.

The main pane displays a list of messages with columns for Subject, Size, Sender, Date, and Order. The messages are all replies to "Anyone notice strange announcements for 174.128.31.0/24". The senders listed include Michienne Dixon, Majdi S. Abbas, Paul Stewart, Josh Karlin, Kevin Oberman, Edward B. DREGER, Randy Bush, and Florian Weimer. The dates are all from 01/12/2009.

At the bottom of the window, the status bar shows: US Pacific: Sun 06:22, GMT/UTC: Sun 14:22, US Eastern: Sun 09:22, Chicago: Sun 08:22, Japan: Sun 23:22, 103 matches found, Unread: 396, Total: 29615.

Threats in BGP routing

- Normal threats
 - Typos – possibly the most common source of bad data
 - Squatters (used to be more common) just pick some space and advertise it.
 - Is it someone else's?
 - Will it eventually be allocated?
 - Doesn't generally matter unless you're assigned a block someone is already using.
 - Spammers
 - Announce, spam, withdraw, move on
 - Malicious DOS
 - Impersonation
 - Could be an active attack, or mostly passive.

DEFCON

In the end, it was hackers at DefCon that got hacked. After three days of software cracking duels and hacking seminars, self-described computer ninjas at the infamous gathering in Las Vegas found out Sunday that their online activities were hijacked without them catching on. (physorg)

Stealing The Internet

An Internet-Scale Man In The Middle Attack

Defcon 16, Las Vegas, NV - August 10th,
2008

Alex Pilosov – Pure Science
Chairman of IP Hijacking BOF
ex-moderator of NANOG mailing list
alex@pilosoft.com

Tony Kapela – Public Speaking Skills
CIO of IP Hijacking BOF
tk@5ninesdata.com



Sexy New threats

(the same ones, only they make the news)

- Youtube hijacking
 - Fat-fingering can be just as destructive as malicious intent
 - Feb 23 2008
 - “Dude, is something wrong with Youtube?”
- DEFCON
 - BGP MITM
 - Put all the the extra pieces together for a low visibility attack on a particular target

Work at filtering out the garbage

- PHAS: Prefix Hijack Alert System took one approach (Lad, Massey)
- PGBGP Efforts (Sriram, Montgomery and Borchert)
 - <http://www.cs.unm.edu/~treport/tr/06-06/pgbgp3.pdf>

Longer Term Community responses security and instrumentation

- Tighten your filters
- Rely more on IRRs
- RPKI
 - SOBGP
 - SBGP
 - SIDR
 - BGPSEC
 - SBGP / SoBGP: What do we Really Need and how do we Architect a Compromise to get it? (Bush, Meyer, Partain, Bellovin Retana 2003)
- Tools developers/realtime

Tighten the filters.

- Easy enough to do for customers and small peers
- Incremental benefit
- Doesn't protect you from people that don't

Rely more on IRRs for prefix validation

- Reliance on IRRs has, if anything gone down.
 - Quality of information present is ambiguous.
- No “License to Route” exists
 - IRRs will allow you to register nearly anything
 - Cooperative approaches are easily abused
 - An ISP that would require an LOA to accept a route from a customer will happily accept it from a peer.
- Filtering complexity grows the closer you are to the “center” of the internet.
- Outside RIPE there's no association between AS and IP prefix allocation.

RPKI

- Resource Public Key Infrastructure
 - Tie ownership of a resource to a trust anchor rooted in PKI.
 - Obviously the RIR's are the right place for the anchors to be.
 - One of the interesting questions is can router's reasonably be trusted with 250k-500k route prefix filter lists for multiple providers
 - Neither soBGP or SBGP are things you can deploy in a production environment.

RPKI continued

- It is highly desirable although not necessarily obvious that you really need to be able to derive incremental benefit from partial deployment of RPKI.

SOBGP

- Protects origin
- Fat Fingers less effective
- Deliberate hijacking, not so much.

SBGP

- Validates the whole path.
- Kind of heavyweight as a result.

SIDR / BGPSEC

- SIDR aiming for origination protection, work ongoing.
- BGPSEC – Doesn't exist.

Tools

- The approach we're using today
- Instrumentation has little effect apart from diagnostic ease on remediation
 - IAR - <http://iar.cs.unm.edu/>
 - PHAS - <http://phas.netsec.colostate.edu/>
 - BGPMON - <http://bgpmon.netsec.colostate.edu/>
 - Cyclops - <http://cyclops.cs.ucla.edu/>
- Real routing intelligence providers
 - Renesys
 - Arbor
 - etc.

Lack of visibility into the routing system

- Does a network participate in the global routing system?
- Are end-users likely to instrument their networks?
 - If it's single homed and takes default from upstream the answer is no.
 - If a network is not participating in the routing system because it's aggregated inside your upstream the answer is no.
- Does that mean the threat can be ignored?
 - Absolutely not.
 - In the meantime it may make it much harder to identify...

Conclusions

- The status quo is not very healthy.
- Experience says RPKI isn't going to get bolted on without external pressure or a massive decline in quality of BGP advertisements.
- Refining your detection model only gets you so far, there are events other than prefix hijacking that are worth noting (peering fights, route optimization software effects etc).

FIN