Short-Lived Prefix Hijacking on the Internet

Peter Boothe[1] James Hiebert[1] Randy Bush[2]

[1]{peter, jamesmh}@cs.uoregon.edu
Computer Science/Computing Center
University of Oregon

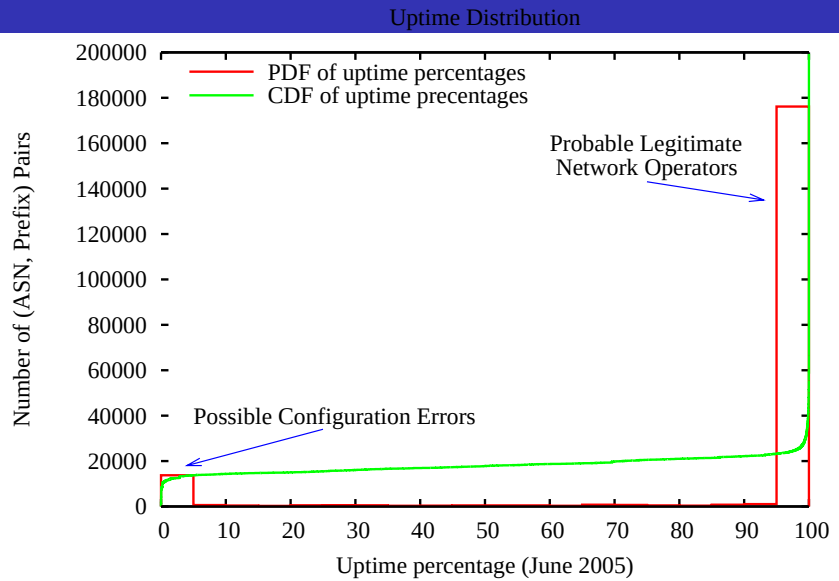
[2]randy@psg.com
IIJ

NANOG 36
February 14, 2006

What Is Prefix Hijacking?

- Announcing space that belongs to someone else without their permission
- Lots of reasons for doing so, almost all of them bad
- Different time-scales of hijackings may be used for different purposes.
- Short lived hijackings are good for getting IP space for spamming, launching attacks, or sharing illegal material anonymously.
- **We are searching for short-lived hijackings**

Short-lived announcements inside a long-lived netblock



- Majority of the AS/prefix pairs are long lasting
- When an AS legitimately controls a netblock, any short lived announcement (by a different AS) inside that block is presumed to be either a misconfig or an invasion
- Announcements at the very beginning of a sample period are also presumed to be legit

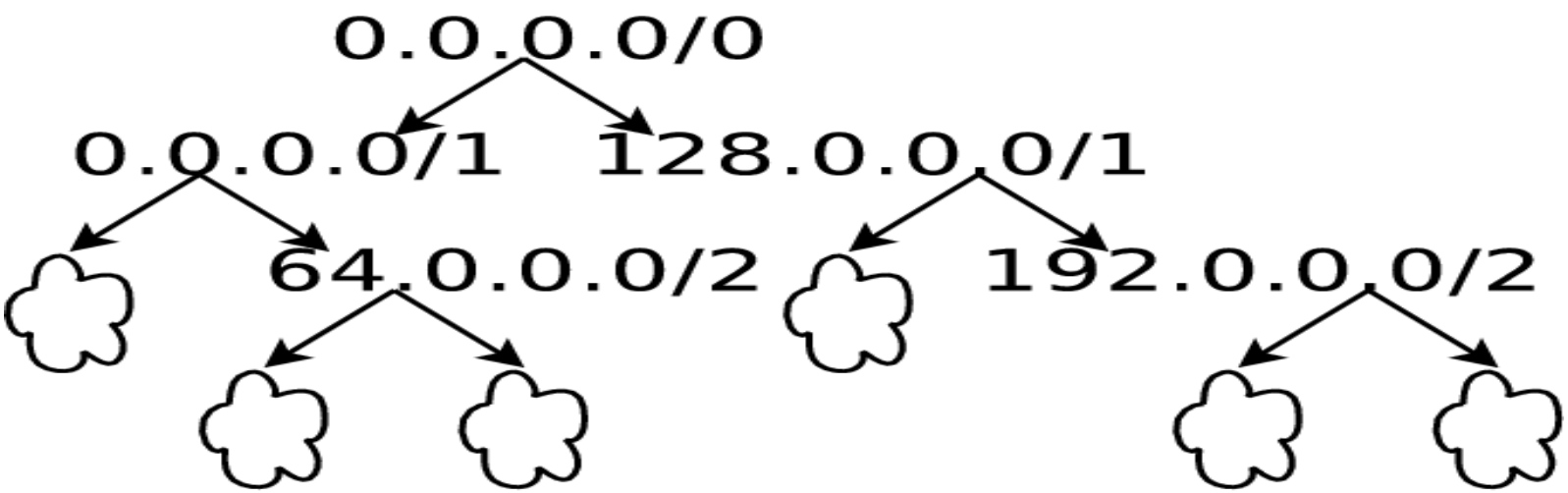
The Routeviews Input Data

- Searched all UPDATE messages in Routeviews data
- Recorded all announced prefixes and the announcing AS

```
TIME: 07/18/07 02:22:29
TYPE: BGP4MP/MESSAGE/Update
FROM: 211.142.32.148 AS12950
TO: 128.223.67.2 AS6337
ORIGIN: IGP
ASPATH: 11956 2114 3657
NEXT_HOP: 211.142.32.148
COMMUNITY: 2914:410 12956:27270 12956:27271
ANNOUNCE
  60.8.238.0/24
  200.21.232.0/24
```

A Tree of the IP Address Space

- All announced netblocks are inserted into a tree
- A list of ASNs which announced the block are recorded at the proper node
- The tree is searched for overlap

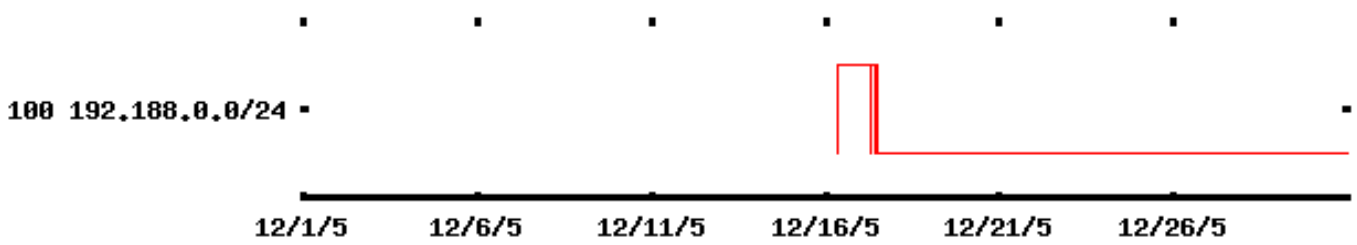


Percent Uptime

- Eliminated all ASN/Prefix pairs with a percent_uptime above a given threshold ($thresh = 90\%$)
- *percent_uptime* defined as:

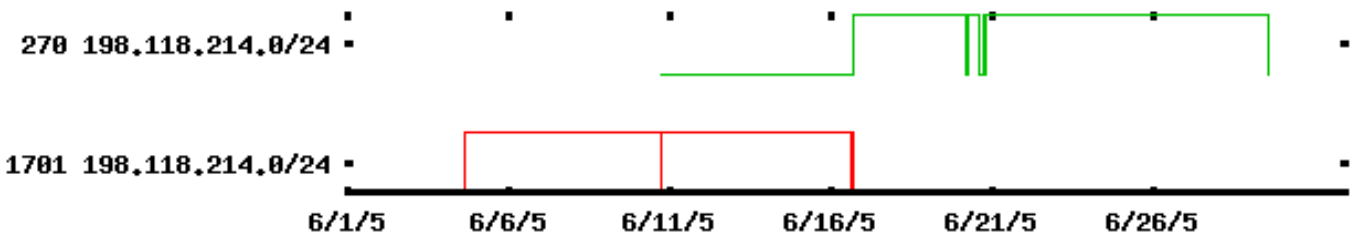
$$\frac{\sum[t_{withdrawal_0} - t_{announcement_0} \ldots t_{withdrawal_n} - t_{announcement_n}]}{t_{endOfMonth} - t_{announcement_0}}$$

- The graphed uptime below would be around 10%



Eliminate Mutually Exclusive Uptimes

- IP space is not always used at same time
- Sometimes prefixes are transferred from one AS to another
- The primary path goes down and their backup strategy involves statically routing through another AS
- Prefixes with mutually exclusive uptimes are eliminated as a possible invasion



Eliminate Customer/Provider Relationships

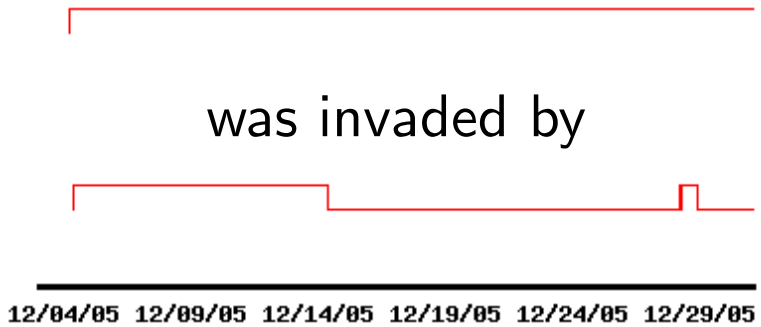
- Final step which is not yet automated
- Manually run a series of tests
  - **AS_OWNS_BLOCK**: Is the entity who owns the AS in whois the same as the entity that owns the netblock in whois?
  - **SAME_AS**: the two ASs in question may be the entity using multiple ASNs; a variety of whois fields can be checked
  - **IMPORT_EXPORT**: some ASs explicitly say in the radb whose paths they import and export; if the invader and the invadee have some relationship, the announcement is more likely legitimate

Final Eliminations

- **INVADEE_ASSIST**: we look at the announcement data and if the invadee passed along the invaded prefix, then it's likely OK
- **FAT_FINGERING**: if the the prefix in question lexicographically similar to something else that AS owns, then do not count the announcement as an invasion

Suspect case: a short lived /24 being used within an unrelated AS

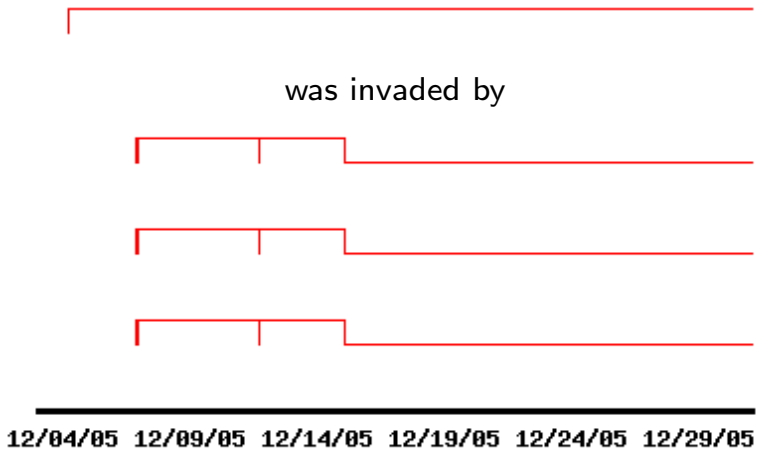
AS	Netblock	Uptime Profile in December 2005
2914	199.224.0.0/20	
		was invaded by
12124	199.224.14.0/24	



- The X-axis is time
- When the line is high, the AS/netblock pair is in the RIB
- When the line is low, the AS/netblock pair has been withdrawn (or the month is over)

Three /24s involved in a probable hijacking

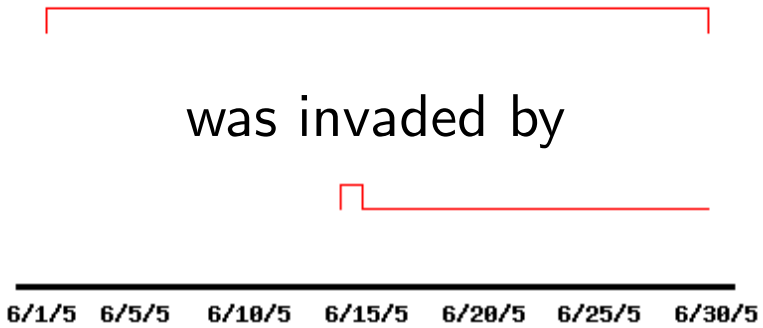
AS	Netblock	Uptime Profile in December 2005
6461	209.249.0.0/16	
		was invaded by
26228	209.249.45.0/24	
26228	209.249.46.0/24	
26228	209.249.47.0/24	



- 26228 is **not** the same entity as 6461
- 26228 is **not** the owner of 209.249.4[567].0/24
- 6461 does **not** have a relationship with 26228 in radb
- 6461 was **not** seen propagating 209.249.4[567].0/24
- The hijacked prefixes are **not** lexicographically similar to 26228's other legitimate prefixes

Fooled by a lag in whois data

AS	Netblock	Uptime Profile in June 2005
701	63.80.0.0/12	
		was invaded by
17284	63.82.77.0/24	



- At the time of announcement 63.82.77.0/24 was not registered as having been sub-allocated
- 17284 announced nothing else in June
- Now whois data indicates that 17284 and the owner of 63.82.77.0/24 are the same entity
- **Detection methods based on whois data will inevitably generate false positives until whois data catches up**

Number of hijackings in December 2005

- Population of 845 ASs which simultaneously announced a prefix inside another AS's, and had a low percent uptime
- Randomly sampled 5% (42 AS-AS invasions)
- Investigated using the previously described manual tests
- 3 were not easily explained as misconfigurations
- Given our entire population, we calculate a *95% confidence interval* of our sample. Result: **between 26 and 95 successful prefix hijackings occurred in December 2005**

For us or others to do...

- Refine search criteria; there's still too much intuition involved
- Automate the remaining manual steps
- Decrease reliance on whois *or* make whois more accurate
- Figure out a way to deal with AS post-pending being (potentially) used to disguise attacks
- What about long term hijackings?

So, to sum up...

- We can identify between 26 and 95 hijacking instances in Route-Views data for December 2005
- Many more misconfigs and false alarms than purposeful hijackings - 750+
- Detection (up to the last step) is automated, but further automation remains dependent on good whois data (hard!)
- We can make code available in any number of ways
- We are willing to make our results, and any future automated results, available to meet the community's needs, via...
  - Biweekly email? - sample email at

    `http://soy.dyndns.org/~peter/ms/presentation/email_sample`
  - Webpage with top 10 lists? - sample page at

    `http://soy.dyndns.org/~peter/ms/presentation/html_sample.html`
  - ...?

Acknowledgments

- NSF Award #0221435
  "Beyond BGP: Flexible and Scalable Interdomain Routing (BBGP)"
- University of Oregon Route Views Project

Questions? Comments?