Detecting Routing Leaks by Counting

Jared Mauch

NTT America

Baseline information

- Analysis done on a RIB snapshot from AS2914
- Also process BGP Updates from archive.routeviews.org
- Uses zebra-dump-parser.pl (modified)
- Store matching data in sql db for queries and history

Technique to detect leaks

- Define a set of major networks, currently:

qwest, ntta, uu, att, xo, level3, cogent, sprint, aol, cw, gx, dt, ft, mfn, teleglobe, telia, tiscali, microsoft, btn, seabone, twtc

```
my @major_network = ("209", "2914", "701",
   "7018", "2828", "3356", "174", "1239", "1668",
   "3561", "3549", "3320", "5511", "6461", "6453",
   "1299", "3257", "8075", "3491", "6762", "4323");
```

Technique to detect leaks

- Undo any sequential prepends, eg: “2914 2914 2914 267” becomes just “2914 267”
- Count the number of $major_network ASNs in the AS_PATH to come up with a score

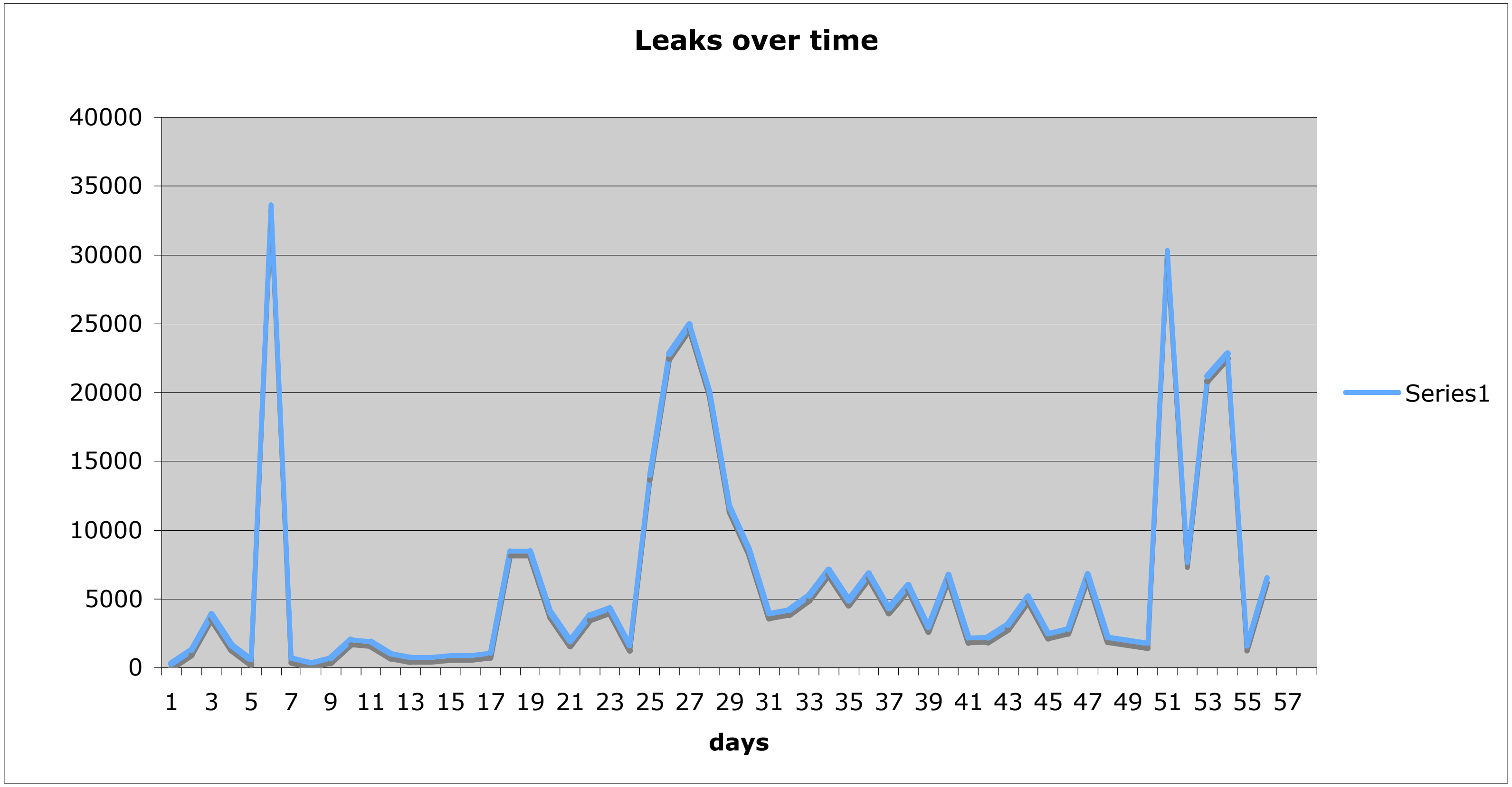
Thresholds

- Default threshold is 2
- Any AS_PATH which exceeds the threshold is likely “bad”
- Known business relationships increase the threshold (~15 currently documented)
- eg: “701 1239 5511” has a score of 3 but threshold is also 3, so will not be flagged

Statistics

- Processing started July 2007
- database archival started in August
- Leak count so far 360,412 (and growing)
- Weekends tend to have less noise
- Slightly over 50% of networks emailed respond and/or fix the issue
  - Language barrier exists with some networks

Graph of leaks per day



“Major Events”

- Aug 25 - 3561 leaked a large number of peer routes
- Oct 12 - 6461 leaked a number of peer routes
- Oct 9 - 7018 routing feed included some “7018 65000 65001 7018” paths

Leaks vs Policy

- Most networks are actually filtering with prefix-lists
- Their customer is multihomed and they leak one transit learned route to another transit
- Outdated prefix-lists
- Lack of an “advanced” routing policy
- Cisco defaults

Downsides to technique

- Found case where a $majornetwork purchased transit. Had to document it for the thresholds
- Blame technique looks for first non-$majornet asn after $majornet series and doesn’t cover enough cases that may require a human to tune/discern

urls and resources

- http://puck.nether.net/bgp/
  - Search the leak history
  - Statistics queries
  - Configuration examples for IOS (juniper coming)
- Email Jared to opt-in for notices
- Coming Soon: (PC accepted the talk too fast)
  - Opt-in for your alerts where you are in the AS_PATH
  - You can either get semi-immediate notices or daily summary

Thanks to

- #ix
- routeviews.org
  - Please feed route-views2 your views as that is the source for the UPDATES
- Everyone who already opted-in and provided feedback

Am I out of time yet?

Questions?

Jared Mauch

jared@puck.nether.net