BGPmon: A real-time, scalable, extensible monitoring system

Dan Massey
Colorado State University

He Yan
Dave Matthews
Kevin Burnett
Colorado State University

Ricardo Oliveira
Lixia Zhang
UCLA
Pakistan Cuts Access to YouTube Worldwide

RIPE NCC:
YouTube reacted about 80 minutes after the Pakistan Telecom announcements, and all the major events finished after about two hours.

Renesys:
This story is almost as old as BGP. Old hands will recognize this as, fundamentally, the same problem as the infamous AS 7007 from 1997, a more recent ConEd mistake of early 2006 and even TTNet's Christmas Eve gift 2004.

Ars Technia:
This vulnerability has been known for a long time, and smaller-scale accidents of this nature happen at regular intervals. But so far, efforts haven't produced any results yet.

03/03/2009
Are You Being Hijacked Right Now?

• 1177 route changes similar to the YouTube hijack occurred in last 24 hours

• And many related problems....
  – Are you unreachable from parts of the Internet?
  – Are your routes stable and reliable?
  – How did the last major cable cut impact you?
Our Two Main Contributions

• Routing Data Needed To Make Decisions
  – Who is originating a route to your system?
  – Which routes changed during some major event?
  – Data from around the globe provided in real-time

• A Prefix Hijack Alert System
  – Digest the data and provide targeted alerts
  – Alarms indicating when you are being hijacked
  – Alert System Available Now
Oregon RouteViews

http://www.routeviews.org
Real-Time Data Access

• Fundamental Changes In Monitoring Infrastructure
  – Provide real-time access to route tables and incremental updates
  – Manage table transfers and update bursts from routers
  – Scale to large numbers of BGP peers
  – Scale to vast numbers of clients
  – Protect monitoring system from slow or misconfigured clients

• Requires Software Dedicated to Monitoring
  – BGPmon: dedicated software for monitoring and real-time delivery
  – XML format for resulting data with integrated updates and tables

• BGPmon overcomes both design and deployment challenges
A Real-Time BGPMonitor (BGPMon)

Internal Dynamic Flow-Control Algorithm
“Push” Data To Clients In Real-Time
XML Merges RIBs, Updates, and Control messages.
Sample Real-Time Data

massey@alpha:~$ telnet bgpdata.netsec.colostate.edu 50001
Trying 129.82.138.6...
Connected to 129.82.138.6.
Escape character is '^]'.
<message>
  <time>2008-09-10T19:09:10Z</time>
  <source_as>3257</source_as>
  <source_ip>89.149.178.10</source_ip>
  <destination_as>6447</destination_as>
  <destination_ip>129.82.138.6</destination_ip>
  <address_family>1</address_family>
  <interface_index>0</interface_index>
  <update>
    <path_attributes><origin><transitive/><igp value='0'/></origin>
    <as_path><transitive/> <as_sequence>3257 3549 6663 35820</as_sequence></as_path> ....snip.... </path_attributes>
    <nlri><prefix label='DPATH'>89.45.4/22</prefix></nlri>
  </update>
  <octets length='77'>FFFFFF...SNIP.... 566B28</octets>
</message>
Message Count From One ISP

The number of messages over time for different types of messages:
- New Announce
- Duplicate Announce
- Same Path
- Different Path
- Withdraw
- Duplicate Withdraw

The x-axis represents time from 09.09.20 to 09.10.18.

The y-axis represents the number of messages from 10 to 1e+06.
## Archived Data Storage Size

<table>
<thead>
<tr>
<th>Format</th>
<th>Uncompressed (Bytes)</th>
<th>/MRT size</th>
<th>Compressed (Bytes)</th>
<th>/MRT size</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRT</td>
<td>26711666</td>
<td>1.00</td>
<td>5614650</td>
<td>1.00</td>
</tr>
<tr>
<td>Bgpdump</td>
<td>74551628</td>
<td>2.79</td>
<td>5645044</td>
<td>1.01</td>
</tr>
<tr>
<td>XML</td>
<td>264824363</td>
<td>9.91</td>
<td>13445451</td>
<td>2.39</td>
</tr>
<tr>
<td>XML-</td>
<td>218065044</td>
<td>8.16</td>
<td>6289003</td>
<td>1.12</td>
</tr>
</tbody>
</table>

XML data requires more space to store, but compresses to nearly match binary format.
BGPmon Queue Management

Queuing and Pacing Algorithms Match Varying Router Write Speeds With Varying Client Read Speeds
BGPMon Queue Implementation

- Warn slowest readers
- Slowest reader loses data if too far behind
Deploying BGPmon Meshes

Robust Mesh Ensures Data Availability
Provides Failure Isolation For Key Users
BGP Deployment Today

- BGPmon1
- BGPmon2
- UCLA Site
- University of Memphis Site
- RouteViews Site
- Cyclops
- Netviews

- 5 routers
- 20 routers
- 6 routers
The Prefix Hijack Alert System

• BGPmon Observes Attacks in Real-time
  • Improve placement to maximize detection
  • Provide real-time (seconds) access to day currently only available after hours.

• But Data Volume is Vast and Growing
  • One collector observes 260,177 prefixes and logged 53,519,042 changes in just a few days!
  • Need smart algorithm to distinguish valid changes from potential attacks
Cyclops: A Network Watchdog

BGPmon provides the raw data
Cyclops alerts you to unexpected behavior

Rules of expected behavior
- Router configs
- Black lists
- Valid prefix lists

Cyclops Engine
- Alarm generation
- Reaction
- False positive detection

Expected

Observed

Network data
- Routing messages
- Geolocation intel
- Active measurement
Using Cyclops (1/2)
Select the Data You Want to Monitor
Using Cyclops (2/2)
Tracks Data and Sends Alerts

My Cyclops

My Prefixes | Add Prefixes | My ASNs | My Neighbors | My Alerts | My Account

Below are the alerts that were created for your account. You can search alerts, close or delete them. Click on alert id for alert details.

Start date: 2009-02-25
End date: 2009-03-04
ASNs:
Prefixes:
e.g. 32.70.18

Alert type: All
Activity: All
Alert status: All

Show my alerts

Total of 4 alerts

<table>
<thead>
<tr>
<th>Alert id</th>
<th>Monitored ASN / prefix</th>
<th>Date (UTC)</th>
<th>Type</th>
<th>Announced prefix</th>
<th>Announced AS path</th>
<th>Duration / Activity</th>
<th>No. monitors</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2880157</td>
<td>52</td>
<td>2009-03-02 20:15:47</td>
<td>new prefix</td>
<td>2607:f0f8::/32</td>
<td>11537 2153 52</td>
<td>00:00:01 / On</td>
<td>1</td>
<td>Open</td>
</tr>
<tr>
<td>2853912</td>
<td>192.35.225.0/24</td>
<td>2009-02-25 02:37:40</td>
<td>next-hop change</td>
<td>192.35.225.0/24</td>
<td>7575 11537 2153 52</td>
<td>00:01:28 / off</td>
<td>1</td>
<td>Open</td>
</tr>
<tr>
<td>2853099</td>
<td>52</td>
<td>2009-02-25 00:51:24</td>
<td>transit</td>
<td>173.0.55.0/24</td>
<td>3130 52 3130</td>
<td>01:27:02 / off</td>
<td>63</td>
<td>Open</td>
</tr>
<tr>
<td>2853104</td>
<td>52</td>
<td>2009-02-25 00:51:24</td>
<td>new neighbor</td>
<td>173.0.55.0/24</td>
<td>3130 52 3130</td>
<td>01:27:02 / off</td>
<td>63</td>
<td>Open</td>
</tr>
</tbody>
</table>
Conclusions

• BGPmon Provides Real-Time BGPdata
  – Essential Data Necessary for BGP Analysis
  – Enables Wide Range of New Services

• Cyclops: Detects Prefix Hijack Events
  – Illustrates power of BGPmon Data.
  – Provides Prefix Hijack Alerts

• Both Services Available Now
Questions