AS-CRED: Reputation Service for Trustworthy Inter-domain Routing

Krishna Venkatasubramanian

Computer and Information Science
University of Pennsylvania

ONR MURI N00014-07-1-0907
Review Meeting
June 10, 2010
Overview

Border Gateway Protocol

Problems with BGP

AS-CRED
  • Behavior Analysis
  • Reputation Computation
  • Alert Generation

Performance Analysis

Conclusion and Future Work
Border Gateway Protocol

AS X
p = 124.0.0.0/8

Address prefix owned by ASX

R1

BGP Update (Announcement)

AS Y

R2

BGP Update (Withdrawal)

AS Z

R3

R4

Autonomous Systems
Problems: Inaccurate BGP Updates

- Announcement of IP prefixes *not owned* by ASX or are *bogons*

- Persistent and well-known problem

- Reasons for occurrence:
  - Blocking Content
    - YouTube was unavailable for about 1 hour when its Prefix was hijacked by Pakistan Telecom AS 17557
  - Spamming
    - AS 8717, an ISP in Sofia, Bulgaria, originated announcements for 82.0.0.0/8
  - May due to malicious intent or misconfiguration

<table>
<thead>
<tr>
<th>Prefix hijacked</th>
<th>Victim AS</th>
<th>Attacker AS</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>63.218.188.0/22</td>
<td>3491</td>
<td>23724</td>
<td>April 8, 2010</td>
</tr>
<tr>
<td>194.9.82.0/24</td>
<td>36915</td>
<td>6461</td>
<td>March 15, 2008</td>
</tr>
<tr>
<td>208.65.153.0/24</td>
<td>36561 (YouTube)</td>
<td>17557</td>
<td>Feb. 24, 2008</td>
</tr>
<tr>
<td>66.135.192.0/19</td>
<td>11643 (ebay)</td>
<td>10139</td>
<td>November 30, 2007</td>
</tr>
<tr>
<td>12.0.0.0/8</td>
<td>7018</td>
<td>31604</td>
<td>Jan. 13, 2007</td>
</tr>
<tr>
<td>82.0.0.0/8</td>
<td>NULL</td>
<td>8717</td>
<td>Dec. 2004 - Jan. 2005</td>
</tr>
<tr>
<td>61.0.0.0/8</td>
<td>4678</td>
<td>17607</td>
<td>Dec. 2004 - Jan. 2005</td>
</tr>
</tbody>
</table>
Problems: Unnecessary BGP Updates

- Repeated announcement and withdrawal of IP prefixes *owned* by ASX, or illegal AS values in update message
- Persistent and *NOT* well-known problem
- Order of magnitude larger problem compared with prefix hijacking
- Principal suspected reason – Misconfiguration of BGP router

- Example:
  - Prefix 41.222.179.0/24 announced and withdrawn 4824 times by AS37035 between Dec. 3, 2009 and Dec. 7, 2009, once every 1.5 minutes.
  - Announcement of private AS numbers (e.g., AS65535) due to improper export policy – filtering

---

Prominent Incidences

<table>
<thead>
<tr>
<th>AS</th>
<th>Prefix</th>
<th>Dates</th>
<th>RAW</th>
</tr>
</thead>
<tbody>
<tr>
<td>7035</td>
<td>41.222.179.0/24</td>
<td>Dec. 3 – Dec. 7 2009</td>
<td>4824</td>
</tr>
<tr>
<td>8452</td>
<td>41.235.83.0/24</td>
<td>Nov. 2 - Nov. 10, 2009</td>
<td>2088</td>
</tr>
<tr>
<td>704</td>
<td>152.63.49.180/30</td>
<td>Dec. 8 - Dec. 31, 2009</td>
<td>1628</td>
</tr>
<tr>
<td>145</td>
<td>140.217.157.0/24</td>
<td>Nov. 1 - Nov. 27, 2009</td>
<td>1080</td>
</tr>
</tbody>
</table>
Approach

• Principal Question:
  – How do we know if ASes are announcing valid updates?
  – Update Validity: necessary and accurate

• Approach:
  – Essentially a question of trust – a subjective expectation on the behavior of an entity
  – In this problem:
    • Entity – Autonomous Systems
    • Behavior – announcement of valid BGP updates

• Observation:
  – ASes repeat their behaviors
  – Past can be used to predict future
  – Metric of choice: Reputation
Goals

1. Compute the reputation for Autonomous Systems in the Internet, by analyzing past BGP updates announced by them for their validity – accuracy and necessity.

2. Provide an alert service for tracking the subsequent announcement of potentially invalid BGP updates based on the computed reputation.

3. Deploy as an publicly available service for everyone to use.
Traditional Approach

BGP Update Invalidity Detection

Prefix Hijacking
- Control-plane Information
  - Karlin et. al 09
  - Qiu et. al 07
  - Lad et.al 04
  - Mahajan et. al 02
  - Xao et. al 02
- Data-plane Probing
  - X. Hu et. al 07
  - Zheng et. al 07
  - Zhang et. al 05
- Reputation
  - N. Hu et. al 07
  - Yu et. al 05

Bogons Private AS Numbers

Frequent Announcements and Withdrawals

Static Checking
- Implemented as a part of BGP route policy space

- Third-Party Feedback Dependent
- Requires Overlay Trust Network

• Use Short-lived prefix announcements as basis for detection
• Consider them both malicious and misconfigured
• Provide alerts for potential hijacks
Traditional Approach

Principal Issues:

- No Non-necessity check
- No quantitative modeling of AS behavior tendencies
- High False Positives

- Use Short-lived prefix announcements as basis for detection
- Consider them both malicious and misconfigured
- Provide alerts for potential hijacks

- Third-Party Feedback Dependent
- Requires Overlay Trust Network

Lad et. al 04
Mahajan et. al 02
Xao et. al 02

X. Hu et. al 07
Zheng et. al 07
Zhang et. al 05

N. Hu et. al 07
Yu et. al 05

BGP route policy space
**AS-CRED: Architecture**

- **BGP Activity Manager:**
  - Database for BGP updates
  - Obtained from well-connected BGP data collectors

- **AS-Behavior Analyzer:**
  - Analyzes the updates in BGP Activity Manager, based on a set of well-defined properties to detect invalidity
  - The results of the analysis, is a feedback on the past behavior of ASes

- **Reputation Manager:**
  - Computes the reputation of the ASes based on a well defined mathematical function
  - Uses past behavior information in the form of feedback

- **Reputation Portal:**
  - Once the AS reputations are computed it is made available through a web portal

- **Alert Manager:**
  - Uses AS reputation, to trigger real-time alerts regarding potential invalidity of any new updates propagated within the Internet.

---

**AS-CRED Architecture**
Data Source: RouteViews

- Basically a group of BGP routers (AS 6447) peered with about 40 other ASes at crucial places
- Receives updates from the peers which it stores in its database without any filtering
- Maintains RIB dumping database: a prefix list with time-stamped information on origin and AS-path
- Route-Views does not originate any prefix or forward a received update message
- RIB dumping every two hours, update messages every 15 minutes
- Useful for analyzing past behaviors of ASes

For every prefix visible to ASes X, Y and Z an entry exists in 6447
Behavior Analysis: Property I

- **Observation**: AS-prefix bindings which are invalid usually last for a short period of time, i.e., they are unstable.

- **Aim**: Detect AS-prefix bindings stability

- **Need**: Historical Information based analysis
  - Analysis window (60 days learning window)
  - Two complimentary metrics
    - Prevalence – percentage of learning window AS-prefix binding lasted
    - Persistence – average time an AS-prefix binding lasted

\[
Pr(p, M) = \frac{\sum_i (Tw^i(p, M) - To^i(p, M))}{T_{learn}}
\]

\[
Ps(p, M) = \frac{\sum_i (Tw^i(p, M) - To^i(p, M))}{N}
\]

AS-prefix binding timeline

<table>
<thead>
<tr>
<th></th>
<th>25%</th>
<th>15%</th>
<th>25%</th>
</tr>
</thead>
</table>

Learning window = 60 days

Pr = 65%; Ps = (0.25+0.15+0.25)*60/3 = 13 days
Property II & Feedback

### Initial Classification

<table>
<thead>
<tr>
<th>Prevalence</th>
<th>Persistence</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hi</td>
<td>Hi</td>
<td>Good</td>
</tr>
<tr>
<td>Hi</td>
<td>Lo</td>
<td>Bad (Unnecessary)</td>
</tr>
<tr>
<td>Lo</td>
<td>Hi</td>
<td>Good</td>
</tr>
<tr>
<td>Lo</td>
<td>Lo</td>
<td>Ugly (Inaccurate)</td>
</tr>
</tbody>
</table>

### Entry format

<table>
<thead>
<tr>
<th>AS</th>
<th>prefix</th>
<th>Timestamp of announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ugly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Good</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Feedback Type

- **Bad**
- **Good**
- **Ugly**

### Refinement

#### Refinement 1
- AS X Ownership of Prefix P
- AS X ownership of Prefix P'
- AS X \( \subset \) P
- Ugly

#### Refinement 2
- Past Ownership and AS_PATH
- AS X \( \rightarrow \) AS W
- Current Ownership and AS_PATH
- AS X \( \rightarrow \) AS W
- AS W \( \rightarrow \) AS Y
- Ugly

#### Refinement 3
- AS X \( \rightarrow \) AS U
- AS W \( \rightarrow \) AS Y
- Ugly
Stability Threshold

- Feedback results in three sets:
  - Good, Bad and Ugly

- Threshold needed to determine:
  - What is Hi and Lo?

- Generated based on comparison with Internet Route Registries (IRR), the closest source to ground truth available

- Compare
  - False Positive: entries in IRR found in Ugly set
  - False Negative: entries not in IRR found in Good and Bad set

- Value of choice: $T_{Pr} = 1\%$ and $T_{Ps} = 10$ hours

Choosing Thresholds
Behavior Analysis: Property II

- **Observation**: BGP updates contain illegal values for ASes and the prefixes they announce
  - Illegal AS numbers:
    - Example, those in the range of: 64496-64511, 64512-65534
  - Bogons:
    - Set of yet to be allocated prefixes

- **Feedback**:
  - Illegal AS numbers:
    - First AS in the AS-PATH with a legitimate value blamed
    - Update considered **Unnecessary**
  - Bogons:
    - The announcer is blamed
    - Update considered **Inaccurate**
Reputation Computation

• AS-CRED computes
  – untrustworthiness of ASes in announcing valid updates
  – Reputation of an AS is computed based on Bad and Ugly feedback only

• Uses a time-decay function where
  \[ Rep_X(a) = \sum_{t_i} 2^{-(t_{now} - t_i)/h_X} \]
  – X is either B or U
  – \( h_X \) is a half-life of behavior X
  – \( t_{now} \) is the current time
  – \( t_i \) is the feedback timestamp:

• Two reputation values created for each AS
  – \( RepU \) – characterizes an AS’s past inaccurate update announcement
  – \( RepB \) - characterizes an AS’s past unnecessary update announcement

• **Half-life:** time by which the weight of the reputation of an AS is halved
  • Set based on by when 75% of the ASes repeat their invalid updates
  • Values: \( h_U = 3 \text{ days} \), \( h_B = 6 \text{ days} \)
Alert Generation Process

Three Steps Process

- **White-List Filtering:**
  - When a new update is received, we first checks to see if its corresponding AS-prefix binding \((a, p)\) is in our white-list \((G\) set)

- **Alert Generation:**
  - If \((a, p)\) are not in the white-list, we post an *potential invalid* Alert

- **Relabeling:**
  - Label updated to *Unnecessary*, if
    - \(\text{RepB}(a)\) is poor or \(\text{RepU}(a)\) is poor with \(p \subset p'\) such that \((a, p')\) is in the white-list.
  - Label updated to *Inaccurate*, if
    - \(\text{RepU}(a)\) is poor with no \(p \subset p'\) such that \((a, p')\) is in the white-list
Behavior Analysis (Nov 1,’09- Dec 30,’09)

- **Property I:**
  - Unnecessary repeated updates far outnumber prefix hijackings or updates with illegal AS numbers
  - Updates for prefix hijacking and illegal AS numbers instances are similar in scale

- **Property II:**
  - 12095 updates affected by illegal AS numbers leading to penalization of 134 ASes
  - Zero instances of Bogons

**Observation:**

- Unnecessary updates a bigger problem in inter-domain routing compared to updates with Inaccurate information

- Repetitive poor behavior displayed, makes reputation a good metric for trust establishment

---

ASes
- Zero instances of Bogons

Shows Number of entries in B and U set after the learning window.
Quality of Behavior Analysis

- **Inaccurate Updates**
  - U set stores instances of inaccurate updates – prefix hijacking
  - Inaccurate updates detected compared with Internet Alert Registry w.r.t. IRR
  - 4 fold improvement in False Positives

- **Unnecessary Updates**
  - B set stores instances of Unnecessary updates
  - Unnecessary updates from repeated announcements and withdrawals were
    - 92% legitimate AS-prefix bindings (based on Internet Route Registry)
    - Announced 42 times more often than Good AS-prefix bindings

### Scheme Analysis

<table>
<thead>
<tr>
<th>Scheme</th>
<th>No Record</th>
<th>IRR Match</th>
<th>No IRR Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS-CRED</td>
<td>841 (13.7%)</td>
<td>975 (18.4%)</td>
<td>4323 (81.6%)</td>
</tr>
<tr>
<td>IAR</td>
<td>4190 (10.7%)</td>
<td>25892 (74.4%)</td>
<td>8903 (25.6%)</td>
</tr>
</tbody>
</table>

### Behavior Analysis (Nov 1- Dec 30) Vs. IAR w.r.t. IRR

- **False Positive Hijack**

### Prominent Examples of Unnecessary Updates

<table>
<thead>
<tr>
<th>AS</th>
<th>Prefix</th>
<th>NAW</th>
<th>Duration Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>8452</td>
<td>41.235.83.0/24</td>
<td>2088</td>
<td>Nov 2-10, 2009</td>
</tr>
<tr>
<td>704</td>
<td>152.63.49.180/30</td>
<td>1628</td>
<td>Dec 8 – 31, 2009</td>
</tr>
<tr>
<td>145</td>
<td>140.217.157.0/24</td>
<td>1080</td>
<td>Nov 1-27, 2009</td>
</tr>
</tbody>
</table>
# Behavior Analysis Overall Statistics

## Prefix Statistics

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes Observed</td>
<td>367605</td>
</tr>
<tr>
<td>SOAS Prefix Observed</td>
<td>357855</td>
</tr>
<tr>
<td>MOAS Prefix Observed</td>
<td>9750</td>
</tr>
</tbody>
</table>

## AS Statistics

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Observed</td>
<td>33925</td>
</tr>
<tr>
<td>AS announcing Unnecessary Updates</td>
<td>1568 (4.6%)</td>
</tr>
<tr>
<td>AS announcing Inaccurate Updates</td>
<td>693 (2.0%)</td>
</tr>
<tr>
<td>AS exclusively announcing Unnecessary Updates</td>
<td>79</td>
</tr>
<tr>
<td>AS exclusively announcing Inaccurate Updates</td>
<td>89</td>
</tr>
</tbody>
</table>

## AS-Prefix Binding Classification

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total AS-Prefix Bindings</td>
<td>376224</td>
</tr>
<tr>
<td>AS-Prefix Bindings in Inaccurate Updates</td>
<td>6139</td>
</tr>
<tr>
<td>AS-Prefix Bindings in Unnecessary Updates</td>
<td>26270</td>
</tr>
</tbody>
</table>

## Behavior Incidences Statistics

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Inaccurate Updates</td>
<td>13615</td>
</tr>
<tr>
<td>Number of Unnecessary Updates</td>
<td>213725</td>
</tr>
</tbody>
</table>
Reputation Analysis

• AS-CRED Reputation characterizes the current perpetrators of invalid updates announcement:
  – ZERO reputation is considered good behavior
  – 693 ASes have $\text{RepU} > 0$
  – 1568 ASes have $\text{RepB} > 0$
  – 90% of ASes with poor behavior have reputation close to ZERO

• ASes show repetitive behaviors
  – Most ASes are good, very few ASes demonstrate repeated poor behaviors

• AS-CRED is sensitive in detecting even announcers of one-off invalid updates
Alert Consistency

- Given AS reputation, newly received updates received over Jan 1, 2010 – Jan 10, 2010 are be evaluated

- Updates not seen in white-list classified as unnecessary or inaccurate based on reputation of announcing AS

- Sets
  - IT - stores all inaccurate updates
  - NN - stores all unnecessary updates

- We use 60 day consistency check window (Nov 20, 2009-Jan 20, 2010) to:
  - Determine if the prediction was accurate
  - Based on behavior analysis

<table>
<thead>
<tr>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total NN set entries</td>
<td>3546</td>
</tr>
<tr>
<td>NN set entries classified in G set</td>
<td>71 (2.5%)</td>
</tr>
<tr>
<td>NN set entries classified in B set</td>
<td>2591 (97.4%)</td>
</tr>
<tr>
<td>NN set entries classified in U set</td>
<td>3 (0.1%)</td>
</tr>
<tr>
<td>Total IT set entries</td>
<td>625</td>
</tr>
<tr>
<td>IT set entries classified in G set</td>
<td>7 (0.2%)</td>
</tr>
<tr>
<td>IT set entries classified in B set</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>IT set entries classified in U set</td>
<td>618 (98.8%)</td>
</tr>
</tbody>
</table>
Alert Accuracy

• For updates deemed inaccurate:
  – AS-CRED detects prefix hijacking in two places:
    • Behavior analysis to populate U set
    • Alert generation when RepU is used to determine if update is a hijack
  – Behavior Analysis shown to be accurate
  – Compared the alert results with Internet Alert Registry and IRR (comparative ground-truth)
  – 8 fold improvement in False Positives

<table>
<thead>
<tr>
<th>Scheme</th>
<th>No Record</th>
<th>IRR Match</th>
<th>No IRR Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS-CRED</td>
<td>112 (18.1%)</td>
<td>42 (8.3%)</td>
<td>465 (91.7%)</td>
</tr>
<tr>
<td>IAR</td>
<td>413 (11.2%)</td>
<td>2437 (75.4%)</td>
<td>798 (24.6%)</td>
</tr>
</tbody>
</table>

• For updates deemed unnecessary:
  – 88% of the associated AS-prefix binding found in IRR
  – Average NAW – 26 with the maximum 4492
  – Contrast for AS-prefix binding in Good set (Avg. NAW ~ 1)
AS-CRED Service Screenshot

WORST PERFORMERS AND REPUTATION STATISTICS

DATE: 19-MAY-2010

Bottom 5 ASes by Reputation

Past Reputation Trend for an AS

Reputation-based Update Alert

http://rtg.cis.upenn.edu/qtm/ascred/

AS REPUTATION SEARCH

SEARCH AS 17557

90 Days RepU Trend

RepU of AS 17557

207.45

90 Days RepB Trend

RepB of AS 17557

255.29

POTENTIALLY INVALID BGP UPDATES

(Latest 5 listed. List updated every hour.)

<table>
<thead>
<tr>
<th>ASN</th>
<th>IP Prefix</th>
<th>Time</th>
<th>Alert Type</th>
<th>RepU</th>
<th>RepB</th>
</tr>
</thead>
<tbody>
<tr>
<td>491</td>
<td>134.135.16.0/20</td>
<td>Wed May 19 23:56:03 2010</td>
<td>Pot. Invalid</td>
<td>0.16</td>
<td>5.89</td>
</tr>
<tr>
<td>491</td>
<td>209.22.19.0/24</td>
<td>Wed May 19 23:56:03 2010</td>
<td>Pot. Invalid</td>
<td>0.16</td>
<td>5.89</td>
</tr>
<tr>
<td>491</td>
<td>140.175.0/16</td>
<td>Wed May 19 23:56:03 2010</td>
<td>Pot. Invalid</td>
<td>0.16</td>
<td>5.89</td>
</tr>
<tr>
<td>491</td>
<td>209.22.18.0/24</td>
<td>Wed May 19 23:56:03 2010</td>
<td>Pot. Invalid</td>
<td>0.16</td>
<td>5.89</td>
</tr>
<tr>
<td>491</td>
<td>209.22.20.0/24</td>
<td>Wed May 19 23:56:03 2010</td>
<td>Pot. Invalid</td>
<td>0.16</td>
<td>5.89</td>
</tr>
</tbody>
</table>

LIKELY INVALID BGP UPDATES

(Latest 10 listed. List updated every hour.)

<table>
<thead>
<tr>
<th>ASN</th>
<th>IP Prefix</th>
<th>Time</th>
<th>Alert Type</th>
<th>RepU</th>
<th>RepB</th>
</tr>
</thead>
<tbody>
<tr>
<td>17557</td>
<td>119.73.35.92/32</td>
<td>Wed May 19 23:33:13 2010</td>
<td>Inaccurate</td>
<td>207.45</td>
<td>255.29</td>
</tr>
<tr>
<td>17557</td>
<td>119.73.180.106/32</td>
<td>Wed May 19 23:32:11 2010</td>
<td>Unnecessary</td>
<td>207.45</td>
<td>255.29</td>
</tr>
<tr>
<td>17557</td>
<td>119.152.21.241/32</td>
<td>Wed May 19 23:01:59 2010</td>
<td>Unnecessary</td>
<td>207.45</td>
<td>255.29</td>
</tr>
<tr>
<td>17557</td>
<td>119.73.35.38/32</td>
<td>Wed May 19 22:03:05 2010</td>
<td>Inaccurate</td>
<td>207.45</td>
<td>255.29</td>
</tr>
<tr>
<td>17557</td>
<td>124.29.192.54/32</td>
<td>Wed May 19 19:34:05 2010</td>
<td>Inaccurate</td>
<td>207.45</td>
<td>255.29</td>
</tr>
</tbody>
</table>
Conclusions & Future Work

• Conclusions:
  – *Repetitive Behavior*: ASes which announce invalid updates do so repeatedly, which makes reputation a good metric to characterize them.
  – *Large number of Unnecessary Updates*: The number of unnecessary updates with poor stability far outnumber the inaccurate ones and those with illegal values.
  – *Sensitivity*: The reputation metric is very sensitive and can capture ASes which seldom announce invalid updates.
  – *Improved Hijack Detection*: The AS-behavior analysis and alert service are much more accurate than existing services (such as the IAR) for detecting prex hijacking.
  – *Consistency of Analysis and Reputation*: The reputation assigned to an AS is a representative and behavior predictive value.

• Future Work:
  – Extend this work by including other properties for determining an AS' tendency to announce valid updates, such as presence of valley-free path and stable links in the AS-PATH.
Thank You & Questions