Resilience of the Internet routing –
a network operator’s view
How “risky” is the global routing system?

How often incidents happen?
- Routing Resilience Measurements Workshop
- Frequency very much depends on the threshold for false positives

What is the impact?
- Data are missing, sensitive or not collected at all
- Risk assessment is a guess at best

Is your network affected?
- Detect incidents
- Eliminate false positives
- Assess the impact

Are you adequately protected?
Routing Resiliency Survey

Introduction

Improving routing security is a key part of ensuring the Internet is a reliable platform for communication around the world. Operational data is an important foundation for monitoring developing trends and making rational decisions to address security issues related to routing. It is also important to measure the effect of routing security tools and technologies once they are deployed. Because the inter-domain routing system is global, such monitoring and measurements should be long-term and be done on a global scale.

However, currently, there is no coordinated approach across network operators to collect or analyze this kind of data, leaving network operators with only incomplete or anecdotal evidence to understand Internet-wide routing security issues.

To address this gap, the Internet Society is inviting network operators to participate in an effort to improve the collection of incident data related to routing resiliency. The effort, undertaken in partnership with the Border Gateway Protocol (BGP) monitoring service BGPmon (http://www.bgpmon.net), also aims to provide a statistically representative picture of these incidents and their impacts, and to provide a basis for risk assessment and global trend analysis. In this context, one important dataset is operational statistics of incidents related to routing security, as registered by a network operator. This survey is aimed at collecting these operational data.

The Survey
Data collection

Network Information
– Once, during the initial sign up.
– Network type, connectivity, and practices used in mitigating routing security incidents. It should take approximately 10-15 minutes to fill out the registration form.

Data related to routing security incidents via an automated monitoring effort
– On first login a “historical” overview will be presented, listing detected suspicious events over last 6-12 months
– After that once a week newly detected suspicious events are collected and displayed in the portal
– Participants are asked to validate and classify these events
  ▪ Impact: severe, moderate, insignificant, not an incident
  ▪ Detection: monitoring system, customer call, this alert
Evidence based risk analysis

<table>
<thead>
<tr>
<th>ID</th>
<th>Alert Type</th>
<th>Your AS</th>
<th>Your Prefix</th>
<th>Detected Prefix</th>
<th>Origin AS</th>
<th>AS Path</th>
<th>Time (UTC)</th>
<th>Seen By Probes</th>
<th>Duration</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>794</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>208.67.220.0/24</td>
<td>208.67.220.0/25</td>
<td>666</td>
<td>1103 271 866</td>
<td>2013-09-19 15:47:35</td>
<td>666 0 active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>734</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>128.189.0.0/16</td>
<td>128.189.128.0/18</td>
<td>393249</td>
<td>28247 262781 28329 12989 271 271 271 393249</td>
<td>2013-06-10 14:15:40</td>
<td>8 22:44:20 active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>735</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>128.189.0.0/17</td>
<td>128.189.96.0/19</td>
<td>393249</td>
<td>34685 11670 13768 271 393249</td>
<td>2013-06-10 14:15:40</td>
<td>7 22:44:20 active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>736</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>207.23.0.0/16</td>
<td>207.23.160.0/19</td>
<td>11105</td>
<td>558 22822 271 11105</td>
<td>2013-04-18 18:58:04</td>
<td>8 22:01:56 active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>737</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>207.23.0.0/16</td>
<td>207.23.192.0/19</td>
<td>11105</td>
<td>40387 11537 6509 271 11105</td>
<td>2013-04-18 18:58:04</td>
<td>18 22:01:56 active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Evidence based risk analysis

<table>
<thead>
<tr>
<th>ID</th>
<th>Alert Type</th>
<th>Your AS</th>
<th>Your Prefix</th>
<th>Detected Prefix</th>
<th>Origin AS</th>
<th>ASPath</th>
<th>Time (UTC)</th>
<th>Seen By</th>
<th>Duration</th>
<th>Status</th>
<th>Classify</th>
</tr>
</thead>
<tbody>
<tr>
<td>794</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>208.67.220.0/24</td>
<td>208.67.220.0/25</td>
<td>666</td>
<td>1103 271 666</td>
<td>2013-09-19 15:47:35</td>
<td>666</td>
<td>0</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>734</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>128.189.0.0/16</td>
<td>128.189.128.0/18</td>
<td>393249</td>
<td>28247 282781 28329</td>
<td>2013-06-10 14:15:40</td>
<td>8</td>
<td>22:44:20</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>735</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>208.67.220.0/17</td>
<td>208.189.128.0/18</td>
<td>458695</td>
<td>271 370 666</td>
<td>2013-06-10 14:15:40</td>
<td>8</td>
<td>22:44:20</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>736</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>207.23.0.0/16</td>
<td>207.23.160.0/19</td>
<td>11105</td>
<td>558 228222 271 11105</td>
<td>2013-04-18 18:58:04</td>
<td>8</td>
<td>22:01:56</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>737</td>
<td>More Specific Announcement by Customer</td>
<td>64500</td>
<td>207.23.0.0/16</td>
<td>207.23.192.0/19</td>
<td>11105</td>
<td>40387 11537 6509 271 11105</td>
<td>2013-04-18 18:58:04</td>
<td>18</td>
<td>22:01:56</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>

Check and Classify
Confidentiality concerns

We understand the sensitivity of some of the data involved in this effort. Therefore, the Internet Society is committed to ensuring participant-specific information remains confidential.

All data collected is stored on Internet Society servers. Any information or analyses shared beyond a specific network will be fully anonymized.
Some statistics: participation

- 4 months
- 24 participants
- 311 networks
- 442 events registered
- 264 events classified
Impact severity
Impact severity (II)

- Severe: 48%
- Moderate: 6%
- Insignificant: 3%
- Unknown: 1%
- Not an incident: 42%
How did you learn about the event?

- NMS Alert
- Customer Call
- RRS Alert
- Not an incident
Interested in Participating?

If you decide to participate, please send a request for the creation of your account to rrs-admin@isoc.org.

In the request please indicate
- your AS number and
- e-mail address for notifications.

You may also include AS numbers of your customers for which you would like to monitor and classify related security incidents.