

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
<http://www.internetsociety.org/doc/report-routing-resiliency-measurements-workshop>
- Frequency very much depends on the threshold for false positives

What is the impact?

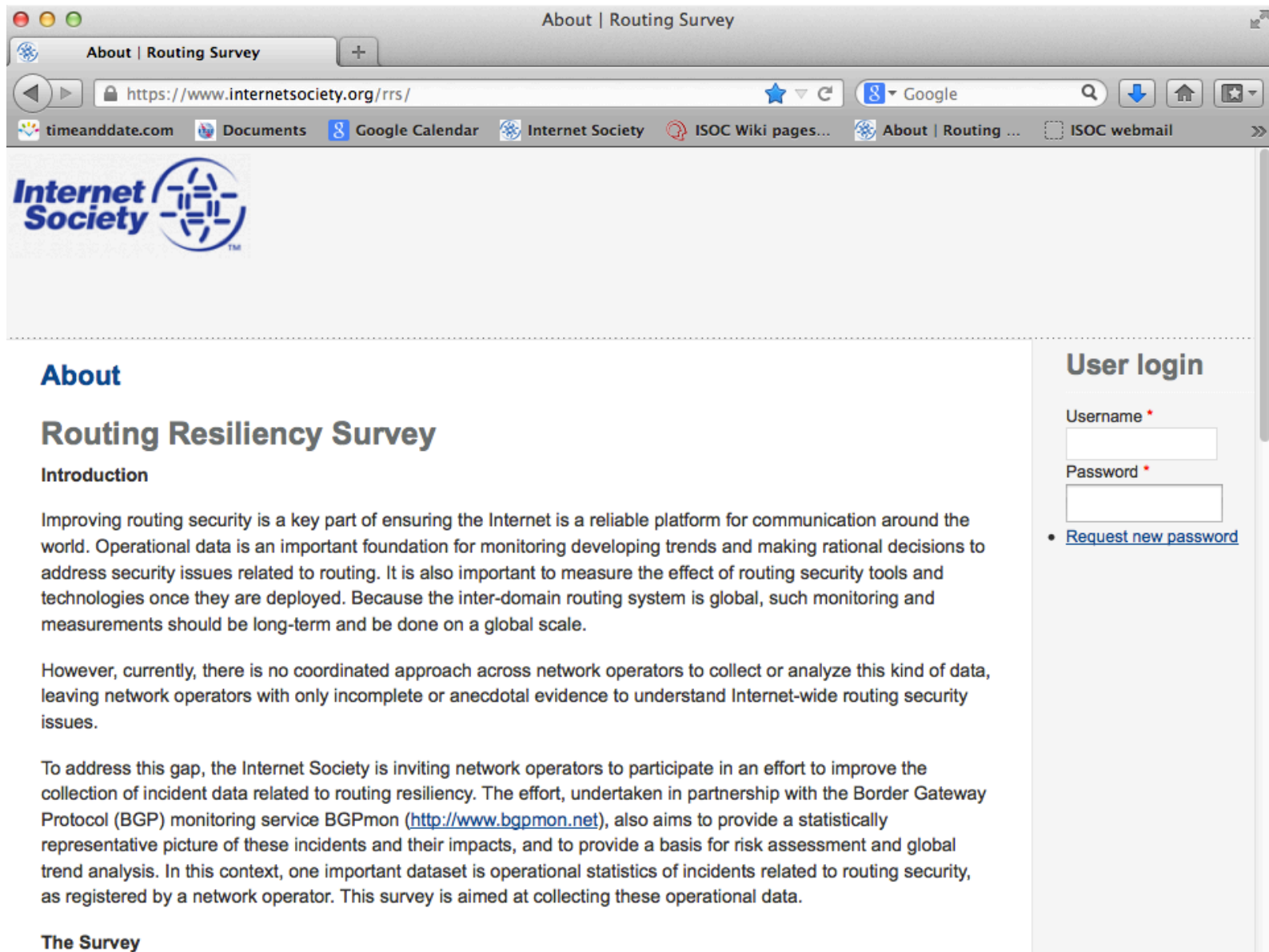
- Data are missing, sensitive or not collected at all
- Risk assessment is a guess at best

Is your network affected?

- Detect incidents
- Eliminate false positives
- Assess the impact

Are you adequately protected?

https://www.internetsociety.org/rrs/



About

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

User login

Username *

Password *

- [Request new password](#)



Evidence based risk analysis

Filter by

Type

Priority
 Critical Warning Notice Info

Include previously classified

Show only Active alerts

Filter

Legend

Critical	Red background
Warning	Yellow background
Notice	Grey background
Info	White background

ID	Alert Type	Your AS	Your Prefix	Detected Prefix	Origin AS	ASPath	Time (UTC)	Seen By #Probes	Duration	Status	Classify
794	More Specific Announcement by Customer	64500	208.67.220.0/24	208.67.220.0/25	666	1103 271 666	2013-09-19 15:47:35	666	0	active	✔
734	More Specific Announcement by Customer	64500	128.189.0.0/16	128.189.128.0/18	393249	28247 262781 28329 2989 271 271 393249	2013-06-10 14:15:40	8	22:44:20	active	➔
735	More Specific Announcement by Customer	64500	128.189.0.0/16	128.189.0.0/16	393249	14695 11370 1376 28329 393249	2013-06-10 14:15:40	8	22:44:20	active	➔
736	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.160.0/19	11105	558 22822 271 11105	2013-04-18 18:58:04	8	22:01:56	active	➔
737	More Specific Announcement by Customer	64500	207.23.0.0/16	207.23.192.0/19	11105	40387 11537 6509 271 11105	2013-04-18 18:58:04	18	22:01:56	active	➔
738	More Specific Announcement by Other AS	64500	206.12.24.0/22	206.12.26.0/24	22950	553 680 20965 6509 26806 22950	2013-02-11 02:40:29	11	14:19:31	active	✔
739	More Specific Announcement by Other AS	64500	206.12.24.0/22	206.12.27.0/24	22950	3367 2603 6509 26806	2013-02-11 02:40:29	11	14:19:31	active	✔

Check and Classify

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

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.

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.