Routing Security Survey: Preliminary Results

Results of a survey during February/March 2010 in the RIPE community, and the IXP communities from AMS-IX, LINX, DE-CIX, and Netnod-IX.
Outline

• Online survey on routing security was part of project commissioned by ENISA
• Results presented are our own first and preliminary observations, interpretations, and conclusions
• Purpose of the presentation
  – feedback to and from the RIPE and IXP communities
  – sanity check of survey outcome
ENISA Background

• Advising and assisting the EU Commission and the Member States on network and information security
• Collecting and analysing data on security incidents in Europe and emerging risks
• Promoting risk assessment and risk management
• Awareness raising and cooperation between different actors in the network and information security field
Goals of Routing Security Survey

• We were interested in:
  – awareness
  – current deployment and experience
  – expectations of (near) future developments
  – policy and governance issues

• Quantitative data from survey can substantiate interviews with routing security experts
Profile of Participants

• More than 130 people from 34 countries responded
  – 80% respondents from EU
    • NW Europe domination: Dutch 24%, Germans 20%, followed by Swedes and other NW Europeans
  – 64% respondents are ISPs
    • other 36% divided among content provider, industry, public body, academic, regulator, and other...
  – experience/responsibilities:
    • 44% technical/operational, 44% strategic/architectural, and 12% policy/managerial level
AWARENESS
Which available technology/methods to improve routing security are you aware of?

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session security (TCP MD5, IPSec, BGP TTL Security Hack, Network Ingress Filtering (BCP 38), etc.)</td>
<td>96,6%</td>
<td>112</td>
</tr>
<tr>
<td>Monitoring and Filtering (IRR/RPSL based filtering, prefix filtering, AS-path filtering, Renesys Routing Intelligence, RIPE IS Alarms–MyASN project, etc.)</td>
<td>87,1%</td>
<td>101</td>
</tr>
<tr>
<td>PKI-based solutions (cryptographic, certification/attestation)</td>
<td>38,8%</td>
<td>45</td>
</tr>
<tr>
<td>Don't know</td>
<td>1,7%</td>
<td>2</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

answered question 116
CURRENT DEPLOYMENT AND EXPERIENCE
Importance of Deploying Routing Security

• How important is deploying routing security in the operation of your organisation?
  – 25% top of the list
  – 63% important, but not a priority
  – 12% not important

• Results consistent with Arbor Networks Infrastructure Security Report
Severity and impact of incidents to the operation of the organisation

Severity of incidents:

- Major disruption to the operation of the organisation
- Minor disruption to the operation of the organisation
- No disruption in the operation of the organisation

Impact to level of awareness:

- Major impact
- Minor impact
- No impact
**What critical risks do you foresee for your organisation in case of breach of routing security?**

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced performance or QoS</td>
<td>69,0%</td>
<td>78</td>
</tr>
<tr>
<td>Reputational damage</td>
<td>77,0%</td>
<td>87</td>
</tr>
<tr>
<td>Loss of money (liability)</td>
<td>43,4%</td>
<td>49</td>
</tr>
<tr>
<td>None</td>
<td>3,5%</td>
<td>4</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>
Which methods are deployed to improve security of inter-domain routing in your organisation?

- **PKI based solutions (cryptographic, certification/attestation)**
- **Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc.)**
- **Session security (TCP MD5, IPSec, etc.)**

Other (please specify)
What is your experience with the methods that you tested or deployed?

- Effective impact
- No observed improvement
- Counter productive
- Didn’t work

Other (please specify)

PKI based solutions (cryptographic, certification/attestation)

Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc.)

Session security (TCP MD5, IPSec, etc.)

n = 77
What are the advantages of the different methods?

- Session security (TCP MD5, IPSec, etc)
- Monitoring & Filtering (IRR/RPSL based filtering, IS Alarms, etc)
- PKI based solutions (cryptographic, certification/attestation)
- Other (please specify)

Ease of deployment
Impact on performance
Don't know
Relative costs of deployment
Effectivity of measure
Risks of mis-configuration
Other

n = 78
FUTURE DEVELOPMENTS
What are the barriers in deploying improved routing security?

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of knowledge</td>
<td>64,9%</td>
</tr>
<tr>
<td>Expected increase in operational costs</td>
<td>45,5%</td>
</tr>
<tr>
<td>Implementation costs</td>
<td>45,5%</td>
</tr>
<tr>
<td>No confidence in their effectiveness</td>
<td>32,5%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>6,5%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>13,0%</td>
</tr>
</tbody>
</table>

n = 77
What are the drivers in deploying improved routing services?

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reducing operational risk</td>
<td>83,1%</td>
</tr>
<tr>
<td>Expected reduction of operational costs (e.g. less ad hoc incident handling)</td>
<td>29,9%</td>
</tr>
<tr>
<td>Improved image towards customers (goodwill, trust, etc.)</td>
<td>59,7%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>5,2%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>6,5%</td>
</tr>
</tbody>
</table>

n = 77
ROLE OF GOVERNMENTS
Should, in your opinion, governments facilitate development and deployment by:

- Incorporation of secure routing requirements in service tender specifications;
- Public R&D investments;
- Legal requirements towards routing security;
- Stimulating self-regulation towards routing security;
- Awareness raising;
- Reconsidering legal restrictions to deployment of secure routing technologies (e.g., use of cryptographic technologies, data protection & privacy);
- Other

![Graph showing percentages of responses for each factor.]

n = 63
Summary

• Routing security
  – session security: MD5, TCP hack, ...
  – monitoring and filtering

• Level of awareness of RPKI is relatively low

• Government involvement: stimulation, not regulation
  – Self-regulation of community is preferred
    • aware of challenges and solutions

  – Stimulating through
    • public R&D
    • awareness raising
With thanks to all that participated

For more information:

maarten@gnksconsult.com
benno@nlnetlabs.nl