NIST
BGP-SRx and BRITE Implementations

BGP-SRx
BGP - Secure Routing Extension

BRITE
BGPSEC / RPKI Interoperability Tester

NANOG 53, October 10, 2011

oliver.borchert@nist.gov

O.Borchert, S.Spies, K.Lee, D.Montgomery, K.Sriram, O.Kim
NIST Tools to Foster RPKI/ BGPSEC Development

• BGP Secure Routing Extension (BGP-SRx)
  – Open source reference implementation for RPKI processing within a router
  – Current stage – Prototype 0.2
    • BGP-SRx Server: Implementation talking to one validation cache using router to cache protocol.
    • BGP-SRx API: Allows integration into BGP routers, policy modules, etc.
    • QuaggaSRx: Integrates BGP-SRx API into Quagga 0.99.16

• BGP RPKI Interoperability Tester and Evaluator (BRITE)
  – Web based system that allows
    • ROA Validation cache
    • BGP router that uses ROA validation results using RPKI to router protocol.
  – Intended for:
    • Users:
      – Test / Experiment with different framework modules (Router / Cache)
    • Software Developer:
      – Run prototypes against and receive reports for debugging
    • Early adapters:
      – Familiarize with RPKI by learning how a system reacts in different situations
BGP-SRx Overview

• **Open Source Reference Implementation**
  – Software router with extensions for: RPKI cache maintenance, ROA and BGPSEC processing of updates, BGP route policies based upon new security tools.
  – BGP Secure Routing Extension (BGP-SRx) is designed as extension for Quagga routing platform. Designed to support other platforms (e.g., XORP, etc.)
  – Designed to support experimentation with different architectural configurations of SRx and RPKI components,

• **Status**
  – BGP-SRx framework with RPKI and ROA processing implemented.
  – Hooks for BGPSEC Path Validation ….
BGP-SRx System Architecture

One BGP-SRx supporting multiple routers

AS 1

One BGP-SRx per router

AS 2

RPKI Validation Cache

BGP Protocol

SRx Router Prot.

BGP Protocol
Quagga SRx Policy Set

- Activation of BGP-SRx Evaluation
  - no srx evaluation
  - srx evaluation (origin_only|bgpsec)

- Ignore Policies
  - [no] srx policy ignore-unknown
  - [no] srx policy ignore-invalid
  - [no] srx policy ignore-undefined

- Local Preference Policies
  - [no] srx policy local-preference valid <int> (add|subtract)
  - [no] srx policy local-preference unknown <int> (add|subtract)
  - [no] srx policy local-preference invalid <int> (add|subtract)

- Prefer Policies
  - [no] srx prefer-valid
BRITE Design Overview

- **IUT**
  - RPKI Validation Cache
  - Origin Validating BGP Router

- **ROA**
  - RSYNC
  - White List Collector / Generator

- **Test Scripts**
  - BRITE Test Controller

- **WEB Interface**

- **Reports / Logs / Traces**

- **Collector**

- **Collector / Generator**
BRITE Overview

• **BGPSEC / RPKI Interoperability Test & Evaluation**
  – Distributed test and evaluation framework for:
    • RPKI / BGP Security implementation testing,
    • Configuration and deployment testing.
  – Flexible XML based test / scenario scripting language.
  – Can test all components / interfaces of BGPSEC system.
    • RPKI Validating Caches.
    • Cache to Router Protocol.
    • ROA Processing in BGP Router.

• **Distributed / automated test system.**
  – WWW interface to BRITE.
  – Multi-user infrastructure.
  – Real time test monitoring & reporting.
  – Other diagnostics – log files, traffic traces available for download.
Intention of BRITE

• BRITE is intended for:
  – Developers of ROA validation / BGPSEC software as test bed.
  – Early adaptors to test the system against.
  – Operators to verify test configuration settings.
  – The operator to be able to evaluate different RPKI/BGPSEC software packets.
  – Researchers to study different behavior and stress test system configurations.
Test Event:
@t1: BGP: AS7 Originates 129.6.0.0/16
@t2: BGP: AS49 Originates 129.6.0.0/16
@t3: RPKI: Add ROA {129.6.0.0/16-24, 49}
@t5: RPKI: Delete ROA {129.6.0.0/16-24, 49}

Test Goals (@collector):
@t1+: G1: BGP Ann. (129.6.0.0/16, AS7)
@t3+: G2: BGP Ann. (129.6.0.0/16, AS49)
@t5+: G3: BGP Ann. (129.6.0.0/16, AS7)
Thank you!

BGP – SRx
http://www-x.antd.nist.gov/bgpsrx

BRITE
http://brite.antd.nist.gov

Questions?
Oliver Borchert (oliver.borchert@nist.gov)
Douglas Montgomery (dougm@nist.gov)
Tests available to the User.

Select a test to be started
BRITE Web Interface (2)

Test Progress

Test Timeline

Events:
M = Multiple
A = Activation
B = BGP
W = Whitelist

Experiment Log

Goal Tree

Wait to be activated
Currently processing
Finished successful
QuaggaSRx (1)

Configuration information related to SRx integration and origin / path processing!
**Update Identifier**

**Validation Result**

**Final(origin, path)**

**Local Preference**

variable (+-) or fixed

---

### QuaggaSRx (2)

```bash
bgpd> show ip bgp
BGP table version is 0, local router ID is 129.6.140.89
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, R Removed
Validation:  v - valid, u - unknown, i - invalid, ? - undefined
SRx Status:  I - route ignored, D - SRx evaluation deactivated
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete
```

<table>
<thead>
<tr>
<th>Ident</th>
<th>SRxVal</th>
<th>SRxLP</th>
<th>Status</th>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 22E78C18</td>
<td>u(u,-)</td>
<td>10.0.0.0</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 359C985B</td>
<td>u(u,-)</td>
<td>10.0.0.0/9</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 7EE7F996</td>
<td>u(u,-)</td>
<td>10.0.0.0/10</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 476AC553</td>
<td>u(u,-)</td>
<td>10.0.0.0/11</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 5011D110</td>
<td>u(u,-)</td>
<td>10.0.0.0/12</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 3470BCD9</td>
<td>u(u,-)</td>
<td>10.0.0.0/13</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 230BA89A</td>
<td>u(u,-)</td>
<td>10.0.0.0/14</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 1A86945F</td>
<td>u(u,-)</td>
<td>10.0.0.0/15</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 76FD453E</td>
<td>u(u,-)</td>
<td>10.0.0.0/16</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 6186517D</td>
<td>u(u,-)</td>
<td>10.0.0.0/17</td>
<td></td>
<td>129.6.141.46</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>i</td>
<td></td>
</tr>
</tbody>
</table>

Total number of prefixes 10
QuaggaSRx (3)

BGP-SRx Information embedded in BGP network information