

BGPsec Interoperability Test QuaggaSRx and BIRD BGPsec

IETF 97

Seoul, South Korea

Nov. 17, 2016

Oliver Borchert

(oliver.borchert@nist.gov)

National Institute of Standards and Technology

Tested Systems:

QuaggaSRx

BGPSEC-IO*

(<https://bgpsrx.antd.nist.gov>)

BIRD BGPsec

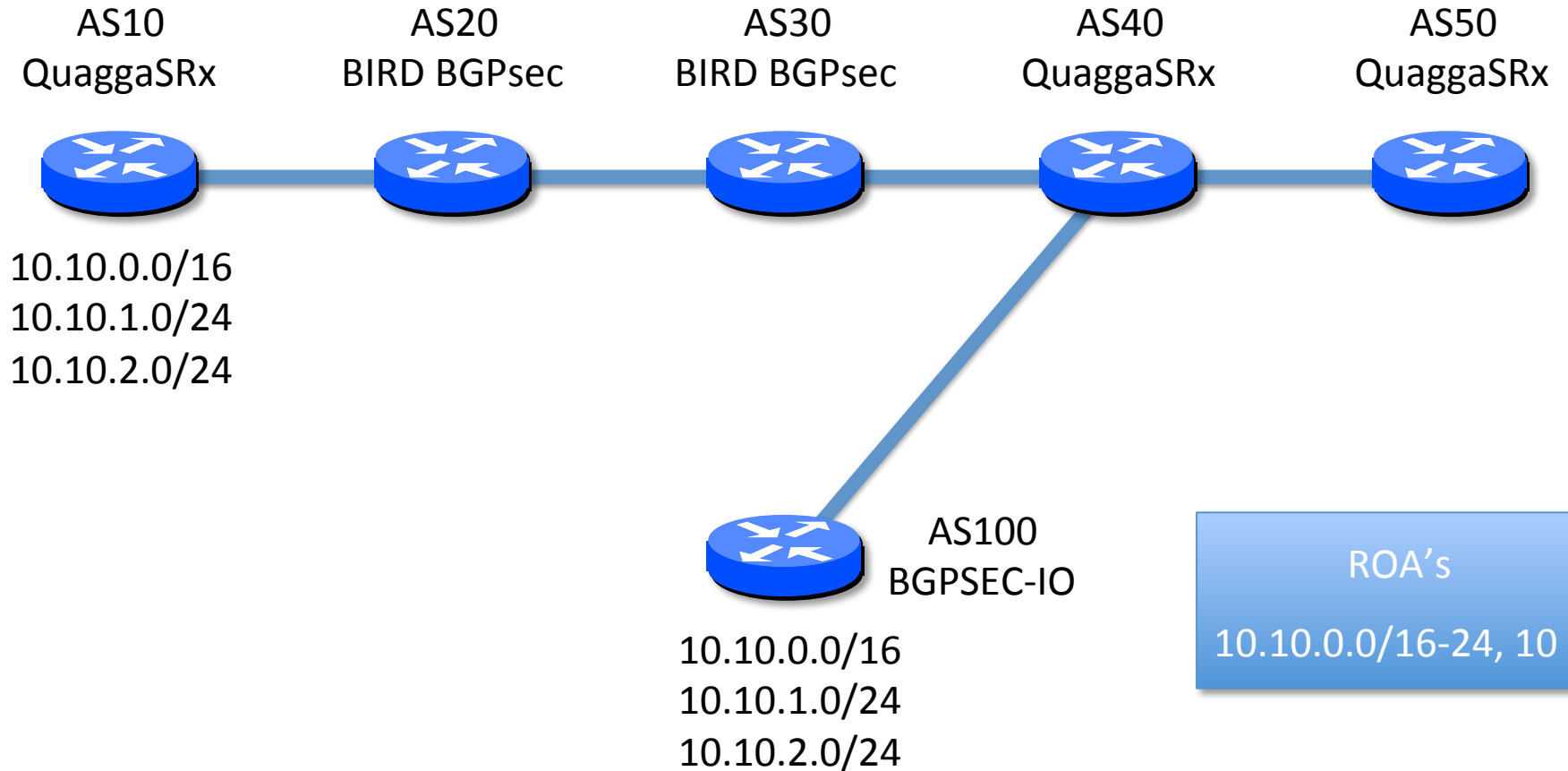
(<http://www.securerouting.net/tools/bird/>)

*BGPSEC Traffic Generator

BGPSEC-IO

- Allows to generate pre-scripted BGPSEC traffic
 - Supports both eBGP and iBGP traffic
 - Allows to display received BGP / BGPsec traffic in “Wireshark” display form.
- Easy to configure
 - Accepts configuration script, command line, piped in traffic.
- Can generate pre-scripted signatures for debugging
- Can test BGPsec crypto modules (SrxCryptoAPI)

Topology Scenario S1



AS100 attempts to hijack the traffic of AS10

Starting AS 10, 20, 30, 40, 50

The screenshot displays a terminal window with five tabs at the top, each representing a different Autonomous System (AS):

- AS10 - QSRx**: [root@AS10 local]# ./run.sh
- AS20 - BIRD**: [root@AS20 local]# ./run.sh
- AS40 QSRx**: [root@AS40 local]# ./run.sh
- AS50 - QSRX**: [root@AS50 local]# ./run.sh
- CACHE**: [admin@AS10 bin]\$./rpkirtr_svr 50000 -f roalist.dat

Below the tabs, there are three main terminal windows:

- AS100 - BIO**: [admin@AS10 bin]\$./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s1
- AS30 BIRD**: [root@AS30 local]# ./run.sh
- TERMINAL AS50**: [admin@CentOS-64 ~]\$ telnet as50 2605

Starting AS 10, 20, 30, 40, 50

```
AS10 - QSRx  AS20 - BIRD  AS40 QSRx  AS50 - QSRX  CACHE
File Edit View Search  File Edit View Search  File Edit View Search  File Edit View Search  File Edit View Search Terminal
0 - ignored  BIRD 1.6.0 ready.  ode: 70 - ignored  10.0.1.64  >>
bird>

AS100 - BIO
File Edit View Search Terminal Help
[admin@AS10 bin]$ ./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s1

AS30 BIRD
File Edit View Search Terminal Help
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24    via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16   via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24   via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>

TERMINAL AS50
File Edit View Search Terminal Help
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete

  Ident    SRxVal SRxLP Status Network      Next Hop      Metric  LocPrf Weight Path
*> F2444D94 v(v,v)      10.10.0.0/16  10.0.1.40      0 40 30 20 10 i
*> 63159BD8 v(v,v)      10.10.1.0/24  10.0.1.40      0 40 30 20 10 i
*> 01072C6F v(v,v)      10.10.2.0/24  10.0.1.40      0 40 30 20 10 i

Total number of prefixes 3
bgpd#
```

Switching to AS40

The screenshot displays a multi-window terminal environment. At the top, five windows are open: AS10 - QSRx, AS20 - BIRD, AS40 QSRx, AS50 - QSRX, and CACHE. The AS20 - BIRD window shows the BIRD daemon is ready. The AS40 QSRx window shows a configuration snippet for AS40. The AS50 - QSRX window shows a configuration snippet for AS50. The CACHE window shows a terminal prompt. Below these, three larger terminal windows are visible: AS100 - BIO, AS30 BIRD, and TERMINAL AS40. The AS100 - BIO window shows a command being executed: `./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s1`. The AS30 BIRD window shows the output of the `show route` command, listing three routes: `10.10.2.0/24`, `10.10.0.0/16`, and `10.10.1.0/24`, all learned via `eth3` from `10.0.1.20`. The TERMINAL AS40 window shows the connection to the AS40 device, displaying the QuaggaSRx version `0.4.2.1` and the copyright information. The prompt is `as40#` and the user is prompted for a password.

```
AS10 - QSRx _ _ x
File Edit View Search
0 - ignored
^
bird>

AS20 - BIRD _ _ x
File Edit View Search
BIRD 1.6.0 ready.
^
bird>

AS40 QSRx _ _ x
File Edit View Search
from 10.0.1.64
^
10.0.1.64
^

AS50 - QSRX _ _ x
File Edit View Search
10.0.1.64
^
>>

CACHE _ _ x
File Edit View Search Terminal

AS100 - BIO _ _ x
File Edit View Search Terminal Help
[admin@AS10 bin]$ ./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s1

AS30 BIRD _ _ x
File Edit View Search Terminal Help
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24      via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16     via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24     via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>

TERMINAL AS40 _ _ x
File Edit View Search Terminal Help
Connected to as40.
Escape character is '^]'.

Hello, this is QuaggaSRx (version 0.4.2.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password: █
```

Switching to AS40

The screenshot displays a network simulation environment with several terminal windows. The top row shows five windows: AS10 - QSRx, AS20 - BIRD, AS40 QSRx, AS50 - QSRX, and CACHE. Below these are three larger windows: AS100 - BIO, AS30 BIRD, and TERMINAL AS40.

The AS30 BIRD window shows the output of the 'show route' command:

```
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24      via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16     via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24     via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>
```

The TERMINAL AS40 window shows the output of the 'show route' command with a table of routes:

```
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Ident	SRxVal	SRxLP	Status	Network	Next Hop	Metric	LocPrf	Weight	Path
*> 09BAC248	v(v,v)			10.10.0.0/16	10.0.1.10	0	0	30	20 10 i
*> 846CC45F	v(v,v)			10.10.1.0/24	10.0.1.10	0	0	30	20 10 i
*> 0D07FE87	v(v,v)			10.10.2.0/24	10.0.1.10	0	0	30	20 10 i

Total number of prefixes 3
bgpd# █

Adding Traffic using BGPSEC-IO

```
AS10 - QSRx
File Edit View Search
0 - ignored
bird>

AS20 - BIRD
File Edit View Search
BIRD 1.6.0 ready.
bird>

AS40 QSRx
File Edit View Search
from 10.0.1.64

AS50 - QSRX
File Edit View Search
10.0.1.64
>>

CACHE
File Edit View Search Terminal

AS100 - BIO
File Edit View Search Terminal Help
[admin@AS10 bin]$ ./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s1

AS30 BIRD
File Edit View Search Terminal Help
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24 via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16 via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24 via 10.0.1.10 on eth3 [bgp2030 00:57:55 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>

TERMINAL AS40
File Edit View Search Terminal Help
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete

Ident SRxVal SRxLP Status Network Next Hop Metric LocPrf Weight Path
*> 09BAC248 v(v,v) 10.10.0.0/16 10.0.1.10 0 0 30 20 10 i
*> 846CC45F v(v,v) 10.10.1.0/24 10.0.1.10 0 0 30 20 10 i
*> 0D07FE87 v(v,v) 10.10.2.0/24 10.0.1.10 0 0 30 20 10 i

Total number of prefixes 3
bgpd#
```

Adding Traffic using BGPSEC-IO

The screenshot displays a network simulation environment with several windows:

- AS10 - QSRx**: Shows a prompt where '0 - ignored' has been entered.
- AS20 - BIRD**: Shows 'BIRD 1.6.0 ready.' and a 'bird>' prompt.
- AS40 QSRx**: Shows a prompt where 'ode: 70 - ignored' has been entered.
- AS50 - QSRX**: Shows '10.0.1.64' at the prompt.
- CACHE**: Shows a 'Terminal' window with '>>' at the prompt.
- AS100 - BIO**: Shows initialization messages:


```
[SRxCryptoAPI - INFO] Extension for private key not set. Set 'der' as key-file extension!
[SRxCryptoAPI - INFO] Extension for public key (X509 cert) not set. Set 'cert' as cert-file extension!
BGP-receiver thread created!
```
- AS30 BIRD**: Shows 'BIRD 1.6.0 ready.' and the output of the 'show route' command:


```
bird> show route
10.10.2.0/24    via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16   via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24   via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>
```
- TERMINAL AS40**: Shows a BGP table with columns: Ident, SRxVal, SRxLP, Status, Network, Next Hop, Metric, LocPrf, Weight, Path.

Ident	SRxVal	SRxLP	Status	Network	Next Hop	Metric	LocPrf	Weight	Path
* 14123092	i(i,v)			10.10.0.0/16	10.0.1.100	0	0	100	?
*> 09BAC248	v(v,v)				10.0.1.10	0	0	30	20 10 i
* 9BBA4C18	i(i,v)			10.10.1.0/24	10.0.1.100	0	0	100	?
*> 846CC45F	v(v,v)				10.0.1.10	0	0	30	20 10 i
* C42630EB	i(i,v)			10.10.2.0/24	10.0.1.100	0	0	100	?
*> 0D07FE87	v(v,v)				10.0.1.10	0	0	30	20 10 i

Total number of prefixes 3
bgpd# █

Adding Traffic using BGPSEC-IO

The screenshot shows a BIRD configuration for AS30 with RPKI and BGPSEC-IO enabled. The configuration includes several 'import' statements for ASNs and their associated IP ranges. The output shows the resulting BGP table with origin and path validation information.

RPKI Origin Validation

BGPSEC Path Validation

Ident	SRxVal	SRxIP	Status	Network	Next Hop	Metric	LocPrf	Weight	Path
* 14123092	i(i,v)			10.10.0.0/16	10.0.1.100	0			0 100 ?
*> 09BAC248	v(v,v)				10.0.1.10	0			0 30 20 10 i
* 9BBA4C18	i(i,v)			10.10.1.0/24	10.0.1.100	0			0 100 ?
*> 846CC45F	v(v,v)				10.0.1.10	0			0 30 20 10 i
* C42630EB	i(i,v)			10.10.2.0/24	10.0.1.100	0			0 100 ?
*> 0D07FE87	v(v,v)				10.0.1.10	0			0 30 20 10 i

Total number of prefixes 3
bgpd#

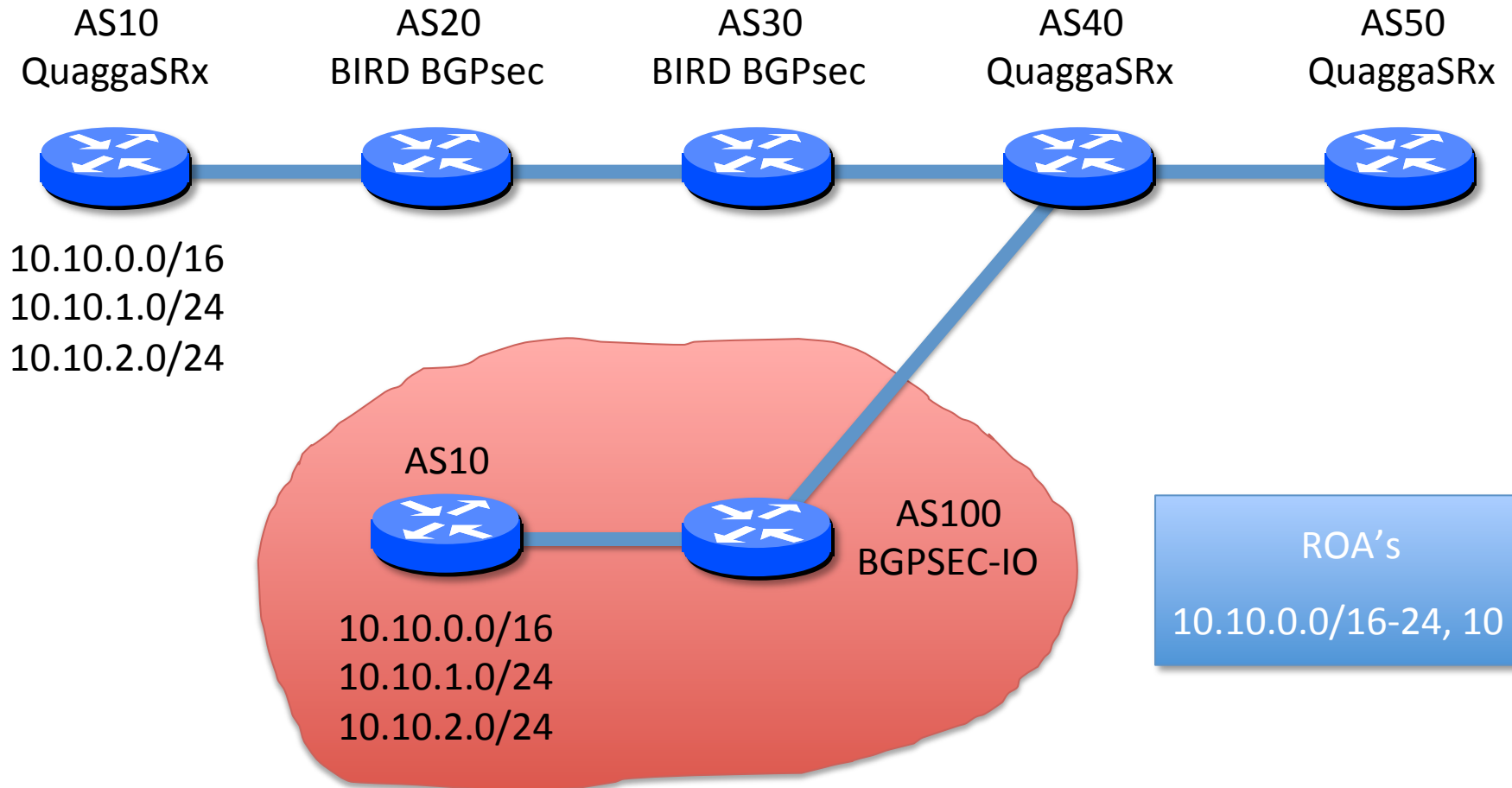
Result

```
* 14123092 i(i,v) 10.10.0.0/16
*> 09BAC248 v(v,v)
* 9BBA4C18 i(i,v) 10.10.1.0/24
*> 846CC45F v(v,v)
* C42630EB i(i,v) 10.10.2.0/24
*> 0D07FE87 v(v,v)
```

```
0 100 ?
0 30 20 10 i
0 100 ?
0 30 20 10 i
0 100 ?
0 30 20 10 i
```

- The Prefix Hijack was unsuccessful:
 - Announced prefixes passed path validation
 - Announcement **failed** RPKI **origin validation**
- Policy is prefer valid
 - no switch to shorter invalid route

Topology Scenario S2



AS100 attempts to hijack the traffic of AS10 by **pre-pending** AS10

Restarting Traffic using BGPSEC-IO

The screenshot shows a multi-windowed terminal environment. At the top, there are five windows: AS10 - QSRx, AS20 - BIRD, AS40 QSRx, AS50 - QSRX, and CACHE. Below these is a window titled AS100 - BIO, which shows the execution of the command `./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s2`. Below that is a window titled AS30 BIRD, which shows the output of the `show route` command. At the bottom is a window titled TERMINAL AS40, which shows the output of the `show route` command, including a table of routes and their status.

```
AS100 - BIO
[SRxCryptoAPI - INFO] Extension for public key (X509 cert) not set. Set 'cert' as cert-file extension!
BGP-receiver thread created!
^C
[admin@AS10 bin]$ ./bgpsecio -f 100-40.bgpsecio.cfg.bgp.s2

AS30 BIRD
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24      via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16     via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24     via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>

TERMINAL AS40
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete

  Ident      SRxVal SRxLP Status Network      Next Hop      Metric  LocPrf Weight Path
*> 3427B993 v(v,v)          10.10.0.0/16 10.0.1.10      0           0 30 20 10 i
*> A86ECF6A v(v,v)          10.10.1.0/24 10.0.1.10      0           0 30 20 10 i
*> A0E53997 v(v,v)          10.10.2.0/24 10.0.1.10      0           0 30 20 10 i

Total number of prefixes 3
bgpd#
```

Restarting Traffic using BGPSEC-IO

```
AS10 - QSRx  AS20 - BIRD  AS40 QSRx  AS50 - QSRX  CACHE
File Edit View Search  File Edit View Search  File Edit View Search  File Edit View Search  File Edit View Search Terminal
0 - ignored  BIRD 1.6.0 ready.  from 10.0.1.64  10.0.1.64  >>
bird>

AS100 - BIO
File Edit View Search Terminal Help
[SRxCryptoAPI - INFO] Extension for private key not set. Set 'der' as key-file extension!
[SRxCryptoAPI - INFO] Extension for public key (X509 cert) not set. Set 'cert' as cert-file extension!
BGP-receiver thread created!

AS30 BIRD
File Edit View Search Terminal Help
BIRD 1.6.0 ready.
bird> show route
10.10.2.0/24    via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.0.0/16   via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
10.10.1.0/24   via 10.0.1.10 on eth3 [bgp2030 01:03:56 from 10.0.1.20] * (100) [AS10i] ASP:2 (BSEC VALID: 20 10)
bird>

TERMINAL AS40
File Edit View Search Terminal Help
  Ident  SRxVal SRxLP Status Network      Next Hop      Metric  LocPrf Weight Path
* 0D345A4C i(v,i)          10.10.0.0/16  10.0.1.100    0          0 100 10 ?
*> 3427B993 v(v,v)          10.10.0.0/16  10.0.1.10     0          0 30 20 10 i
* C8CEB9F1 i(v,i)          10.10.1.0/24  10.0.1.100    0          0 100 10 ?
*> A86ECF6A v(v,v)          10.10.1.0/24  10.0.1.10     0          0 30 20 10 i
* A637BD2C i(v,i)          10.10.2.0/24  10.0.1.100    0          0 100 10 ?
*> A0E53997 v(v,v)          10.10.2.0/24  10.0.1.10     0          0 30 20 10 i

Total number of prefixes 3
bgpd#
```

Restarting Traffic using BGPSEC-IO

The screenshot shows a BIRD terminal window with several windows open: AS10 - QSRx, AS20 - BIRD, AS50 - QSRX, and CACHE. The main terminal window displays the following output:

```

[SRxCryptoAPI - INFO] Extension for private key file extension!
[SRxCryptoAPI - INFO] Extension for public key file extension!
BGP-receiver thread created!
* 0D345A4C i(v,i) 10.10.0.0/16
*> 3427B993 v(v,v)
* C8CEB9F1 i(v,i) 10.10.1.0/24
*> A86ECF6A v(v,v)
10.10.2.* A637BD2C i(v,i) 10.10.2.0/24
10.10.0.*> A0E53997 v(v,v)
10.10.1.*
bird>
  
```

Callouts highlight the following features:

- RPKI Origin Validation**: Points to the RPKI-related configuration and output.
- BGPSEC Path Validation**: Points to the BGPSEC-related configuration and output.

The terminal also shows a table of BGPSEC-IO output:

Ident	SRxVal	SRxIP	Status	Network	Next Hop	Metric	LocPrf	Weight	Path
* 0D345A4C	i(v,i)			10.10.0.0/16	10.0.1.100	0	0	0	100 10 ?
*> 3427B993	v(v,v)				10.0.1.10	0	0	0	30 20 10 i
* C8CEB9F1	i(v,i)			10.10.1.0/24	10.0.1.100	0	0	0	100 10 ?
*> A86ECF6A	v(v,v)				10.0.1.10	0	0	0	30 20 10 i
* A637BD2C	i(v,i)			10.10.2.0/24	10.0.1.100	0	0	0	100 10 ?
*> A0E53997	v(v,v)				10.0.1.10	0	0	0	30 20 10 i

Total number of prefixes 3
bgpd# █

Result

* 0D345A4C i(v,i)	10.10.0.0/16	100 10 ?
*> 3427B993 v(v,v)		30 20 10 i
* C8CEB9F1 i(v,i)	10.10.1.0/24	100 10 ?
*> A86ECF6A v(v,v)		30 20 10 i
* A637BD2C i(v,i)	10.10.2.0/24	100 10 ?
*> A0E53997 v(v,v)		30 20 10 i

- The Prefix Hijack was unsuccessful:
 - Announced prefixes **failed path validation**
 - Announcement passed RPKI origin validation
- Policy is prefer valid
 - no switch to shorter invalid route

Questions ?



oliver.borchert@nist.gov

National Institute of Standards and Technology