RQspec

improved tooling for routing security

Rüdiger Volk, Deutsche Telekom Technik GmbH
still <rv@NIC.DTAG.DE>

NANOG 78
February 2020, San Francisco

Outline

- one factor of routing security: manage rigid ingress route filters!

- route (prefix) filtering and documentation - based on what data?

- RQspec query specification, details, web portal for diagnostic evaluation

- snapshots of diagnostic data presentation

problem space – traditional

- document customer cone by AS-set in IRR

- register route[6]:s in IRR

- which IRR? quality in IRR? authorization?

- to avoid garbage be very selective in IRR use

- do we have commonly understood, precise specification for using IRR to evaluate customer cone route-set for prefix filter?

- diagnostics to help identify trouble spots in your customer cone IRR data?

now look at RPKI

- RPKI ROAs as new data set – looks like clean, authorized source route[6]: info!

- can we focus adding new documentation into RPKI and avoid redundant copies spread in IRR? (focus learning on new&good system!)

- … and make best use of both old IRR and new RPKI information?

to help RQspec…

- provides exact and complete specification for how to evaluate the routing policy databases for your customer cone (AS=>routes) [to be used for filtering your announcements]

- allows to make full combined use of IRR/RPSL and RPKI/ROA information and enables smooth progress towards the authorized new system

- is implemented as command line tool (used in generating configs)

- and available as a web based services

  - with API for tool integration

  - and extended web pages to support diagnostic use (also for customer use)

- and provides extra evaluation modes (variants) that help to analyze and diagnose data quality

- … certainly some other tools will be useful for analysis and diagnosis

RQspec: specify **Q**ueries for **R**outing documentation/filter data

- uses underlying XML schema (hidden by web UI)

- XML/XSLT rule set for generating unambiguous RPSL object name for results and the commands for evaluation process (using our IRRtoolSet derivative *irreval*)

- web pilot use internally with DT subsidiaries, ongoing improvements

- … public service would seem useful
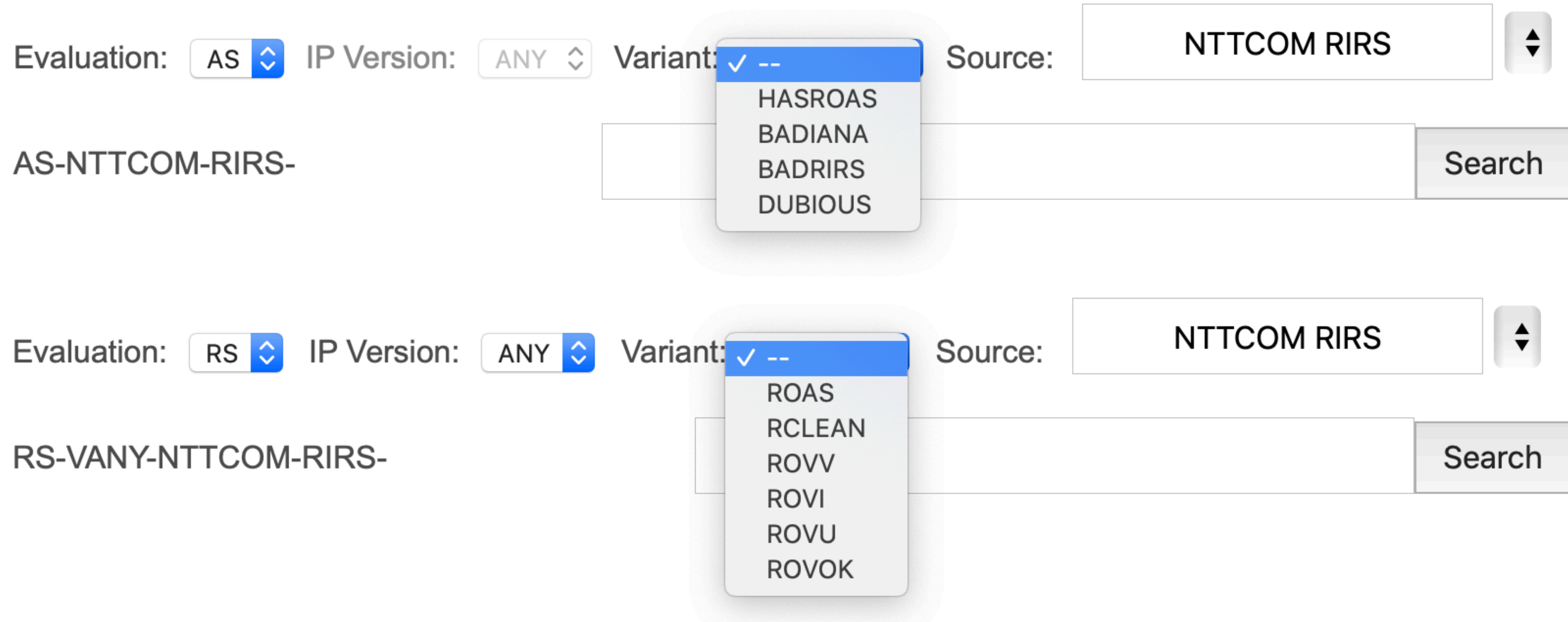
schema components/web UI

RQspec Sets

Enter an AS or an AS-Set name, select the IRR database it can be found in and the type of set you want, then hit 'enter' or the submit button. The set is then retrieved and displayed with its full name. In case you know the full name of the set you want, there is a page where you can enter it directly.

Evaluation: [AS ⇅]   IP Version: [ANY ⇅]   Variant: [✓ --   HASROAS   BADIANA   BADRIRS   DUBIOUS]   Source: [NTTCOM RIRS ⇅]

AS-NTTCOM-RIRS-   [   ]   [Search]

Evaluation: [RS ⇅]   IP Version: [ANY ⇅]   Variant: [✓ --   ROAS   RCLEAN   ROVV   ROVI   ROVU   ROVOK]   Source: [NTTCOM RIRS ⇅]

RS-VANY-NTTCOM-RIRS-   [   ]   [Search]

variants for AS-set

- default: IRR = plain IRR

- BADIANA: AS not allowed by IANA for regular use

- BADRIRS: AS not allowed by RIRs (free pool, blocked, …) according to NRO provided data set with daily updates

- DUBIOUS: collection of AS usually not expected in customer cones (such as tier 1)

- HASROAS: for curiosity does RPKI have ROAs for AS?

variants for route-set

- default: plain IRR

- ROAS: only RPKI ROAs (for resolved IRR AS-set [customer cone])

- classify IRR routes using RPKI origin validation

  - ROVI   **invalid**

  - ROVV   **valid**

  - ROVU **unknown** (excludes both ROVI and ROVV!)

  - ROVOK   **acceptable** (valid or unknown)

- **RCLEAN: combined clean** IRR (i.e. *invalids* removed) and RPKI information (i.e. ROAs added)

"customer" analysis web presentation

- required input:

  - AS-set name (for customer cone)

  - IRR sources to use

- evaluates all RQspec variants and provides tables for

  - AS-set evaluation

  - route-set evaluation

- see next slides

AS-set variant diagnostic table

T···DTAG IRR Data

Source: **AS or AS Set:**

RIPE   ⬍   AS-MTNET   Submit

AS3320:AS-RIPE-AS-MTNET and Variants

(members: 54 · from 11.2.2020, 10:23:00 · duration: 7.07 sec) Refresh

Member	IRR	HASROAS	BADIANA	BADRIRS	DUBIOUS
54	54 ☐	16 ☐	0	1 ☐	0
AS1299	IRR	HASROAS			
AS5379	IRR				
AS6821	IRR				
AS8830	IRR				
AS8982	IRR				
AS9119	IRR	HASROAS			
AS16333	IRR	HASROAS			
AS16477	IRR				
AS21183	IRR	HASROAS			
AS49056	IRR				
AS49094	IRR			BADRIRS	

planning progress:
switch default for filter generation to RCLEAN

- help to use RPKI for authorization/documentation without redundant RPSL route[6]: documentation

- IRR/RPSL AS-sets still needed to document customer cones :-(

  - essentially no security possible; tends to accumulate garbage

- RPKI not really appropriate for customer cone AS-sets

  - but RPKI ASPA under development for AS relation documentation – actually allows authorization/security; works the opposite direction compared to AS-set (RPSL/AS-set emulation of ASPA is possible before RPKI/ASPA operational)

Credits

- RQspec (XML/XSLT processing, web frontend)

  - greenbytes.de

- preparing data (RPKI, NRO): Frank Endemann

- irreval for all the extended RPSL handling

  - IRRtoolSet

  - Michael Müller

  - Hagen Böhm

  - RTRlib (http://rtrlib.realmv6.org/, FU Berlin & HAW Hamburg)