



Monitoring, Testing, and Deployment of RPKI Using RTRlib and RPKI MIRO

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

RTRlib: In a Nutshell

General objective

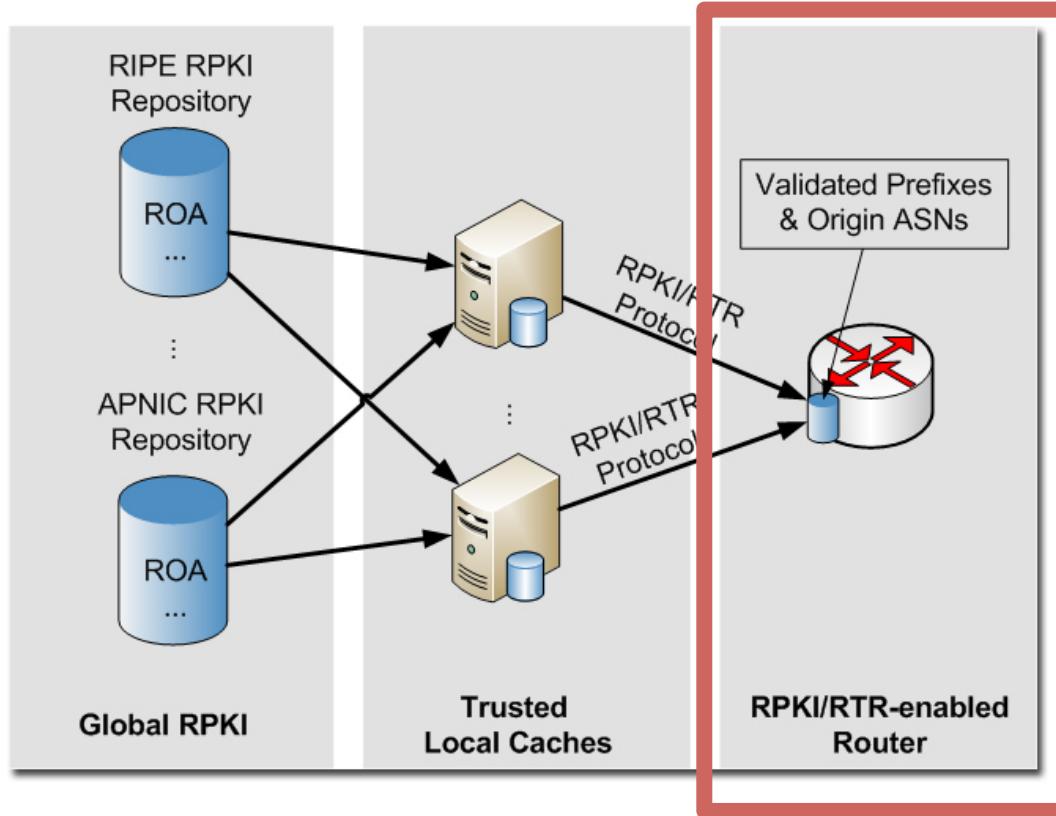
- Highly efficient implementation of RPKI-RTR client protocol
- C library for RPKI prefix origin validation

Details

- Fetch validated prefixes + origin ASes from RPKI cache
- Keep the routers validation database in sync
- Provide an interface between local database and routing daemon to access validated objects
- Allow also for validation of BGP updates
- Fully compliant with all relevant IETF RFCs/drafts

It's open-source!
<http://rtrlib.realmv6.org>
<https://github.com/rtrlib/rtrlib/>

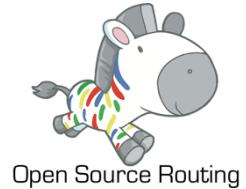
RTRlib in the RPKI Architecture



Applications Using RTRlib

Open Source BGP Daemons + RPKI Origin Validation

- Quagga
 - Fork will be integrated in the master branch soon
- BIRD
 - External CLI, as well as
 - Integration in main BIRD source code, should be available w/ next release



Example Monitoring Tools

- REST BGP RPKI Validator
- RPKI Web Browser Plugin
- Support in CAIDA BGPStream
- Advantage using RTRlib underneath:
Independent of specific cache server



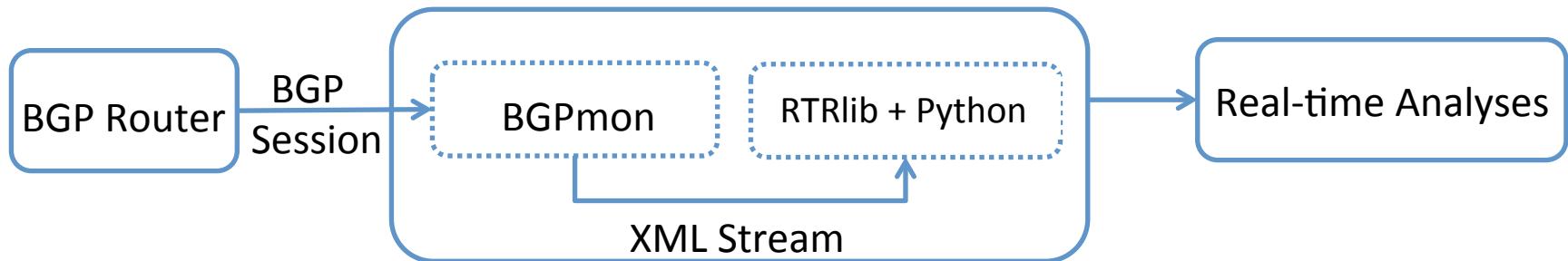
RTRlib: Live Monitoring of Origin Validation

Objective: Emulate origin validation of your BGP peer

Setup – No Firmware Changes at Your Router:

- Tools: RTRlib + Python Script + BGPmon
- Establish peering between your router and BGPmon

Demo
<http://rpki-read.realmv6.org>



RPKI MIRO: In a Nutshell

General objective

- Monitoring and Inspection of RPKI Objects

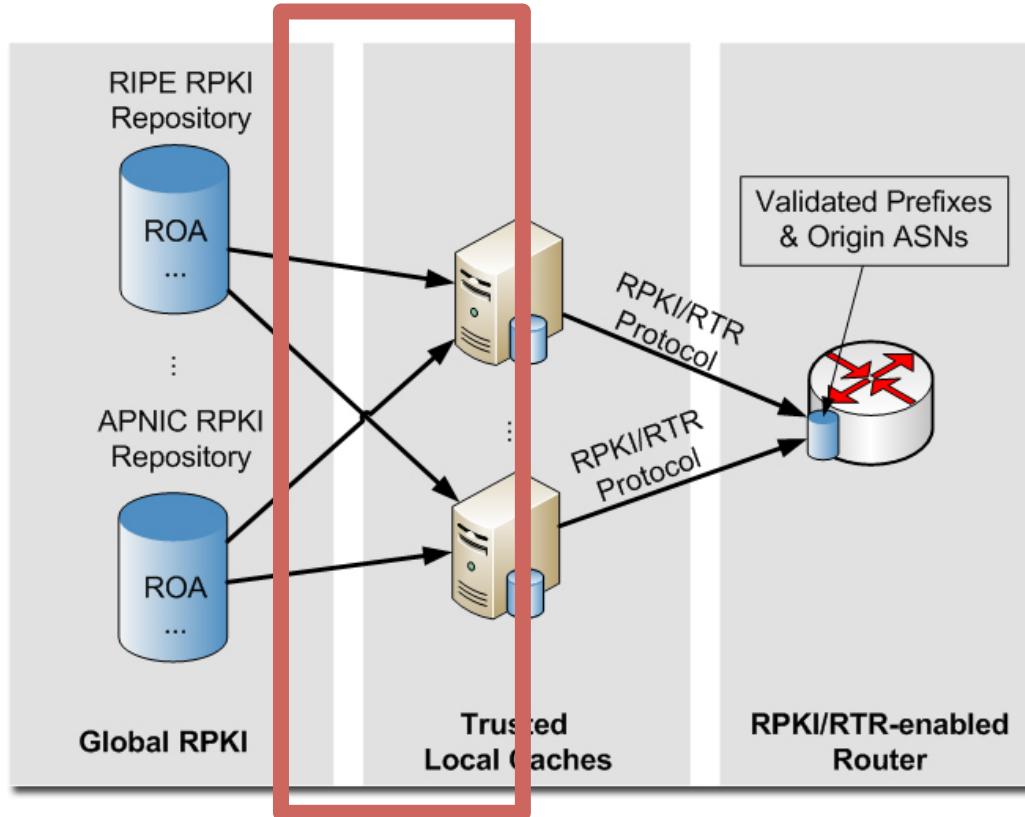
Details

- Functions to collect RPKI data from remote repositories
- An intuitive browser to visualize RPKI objects
- Statistical analysis of the collected objects.

It's open-source!

<http://rpki-miro.realmv6.org>
<https://github.com/rpki-miro/>

RPKI MIRO in the RPKI Architecture



RPKI MIRO: Browser

RPKI Repository Browser RPKI Browser Statistics About

Filter Clear Filter List View RIPE

Certificate Manifest CRL

2015-03-15 20:34:44.000448 UTC

ripe-ncc-ta.cer

- b1314c89c8803a127d62c83f01292a0474b
 - 102ed0852ea4b4700eaef91a42e9f7e0fe5349
 - a4250f3c598917bc119f7ddd423595bb7251181c
 - CnL-b5z5_hDy2tW1BsZhKuG21hYcer
 - j86YvmixvIDi5KNK_9WRWSkk.cer
 - AndpRricSnpJmEqYZgbTkE9dqO8.cer
 - XlUMPPD4fBE_q7YLpzzk4Veis.cer
 - X3qXC5SuxplvEvylMyo4CReyl-4.cer
 - jSvd3GcxMvclDgsa6pNVtV1_v1w.cer
 - 1JEExgH74Hry26tqz6rGl2p4R28.cer
 - NtmoRku7irFWj90V4aAdDNTs5IU.cer
 - aa2304f03c4e807dae51fd33008c93692b973c
 - Ruc65KpbfQGAQydQ7x5ol_lVgQ4.cer
 - XV0MrctsyqyGzbKnWjZJmY2g-Fw.cer
 - QeQtMzC4g6BT-HwyJuRaHoOf58.cer
 - VaXbVKUQriSTAWB1uCg63QPXewU.cer
 - waUAp3G0Emk_0Af2gP_UBG0RteY.cer
 - knMd92pdnJe2c9b8inSlWUryp5o.cer
 - mkOLG21dav_HKJfom0zh117EjHI.cer
 - QQhCRmuWm57zZEGLoft_SLtuyi8.cer
 - uM4Xr2ldvSDL6.JpNYAf6JmKJ18.cer
 - ZGd0ksxSG3BzQpc70U53CWT1hQg.cer
 - PyDHy3BMKMFjsNglyV7gC6Mfk.cer
 - PkRGD2o_FemnU27kMFKA4Q0T7ys.cer

Validation Status: PASSED

Validity Period: 2015-02-20T12:46:54.000Z - 2020-02-20T12:46:54.000Z

Errors: None

Warnings: None

Subject: CN=a4250f3c598917bc119f7ddd423595bb7251181c

SKI: A4250f3c598917bc119f7ddd423595bb7251181c

Issuer: CN=ripe-ncc-ta

AKI: E8552B1FD6D1A4F7E404C6D8E5680D1EBC163FC3

SerialNr: 114

Filename: a4250f3c598917bc119f7ddd423595bb7251181c.cer

Location: rsync://rpki.ripe.net/repository/

EE: false

CA: true

TA: false

Public Key:

```
Sun RSA public key, 2048 bits
    modulus: 2659754460864297460260769704493764420384535607017889082384001
    2333166328324581714113271806374028960256665454092340053165110993121659
    114300800531649290096624936758644154231824703175653701760197647147810224
    8596103127881117179329004902453924452251840880045378255876124861486506
    029861129042039330388302765453520628000748943233695002957117146430838158
    502965676125390423306254418337804924235488959512524903372188967718146330
    6546206761977270530376717032172723123786833585401949433559592278004
    1225121555846848978369981813880958154897166165935777384849941625660028077
    0982845189497090885051248072528001183318691
    public exponent: 65537
```

[ASCII download](#)

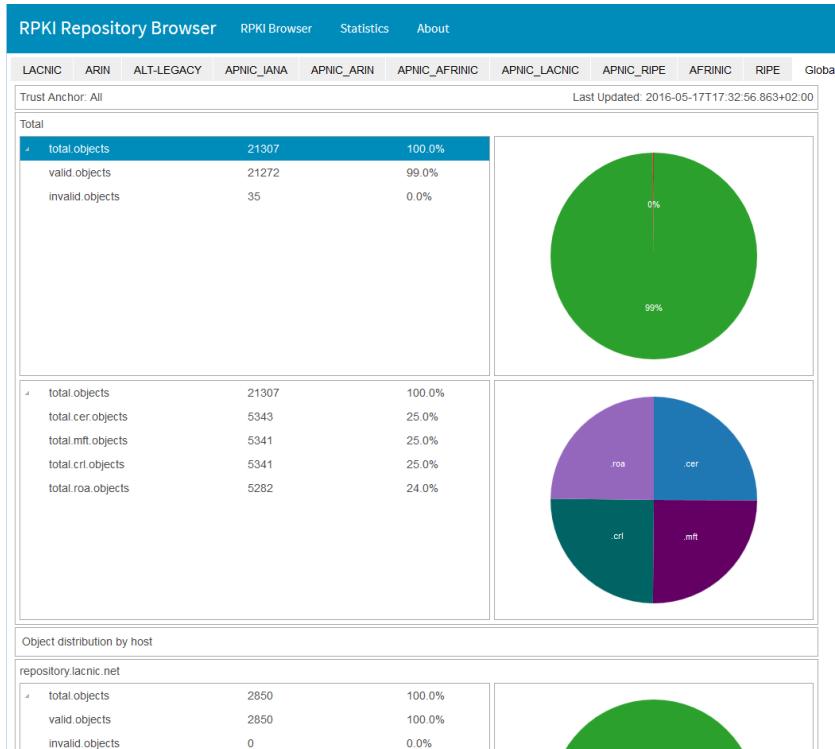
Resources

- 150.106.0.0/16
- 150.128.0.0/16
- 150.132.0.0/16
- 150.140.0.0/16
- 150.145.0.0-150.146.255.255
- 150.158.0.0/16
- 150.175.0.0/16
- 150.178.0.0/16
- 150.204.0.0/15
- 150.213.0.0-150.214.255.255
- 150.217.0.0/16
- 150.227.0.0/16
- 150.236.0.0/15
- 150.241.0.0/16
- 150.244.0.0/16
- 150.251.0.0/16
- 150.254.0.0/16
- 153.1.0.0/16
- 153.5.0.0/16
- 153.15.0.0/16
- 153.17.0.0/16

Try it!
rpki-browser.realmv6.org

RPKI MIRO: Stats

- RPKI MIRO allows for distributed RPKI probes
- Fetching RPKI objects
 - Currently, only rsync support
 - Support for delta protocol on the way
- We can add your CA, let us know!



Contact

RTRlib (and integrations in Quagga, BIRD, and CAIDA BGPSStream)

- <http://rtrlib.realmv6.org>
- <http://rpki-read.realmv6.org>
- <https://github.com/rtrlib>



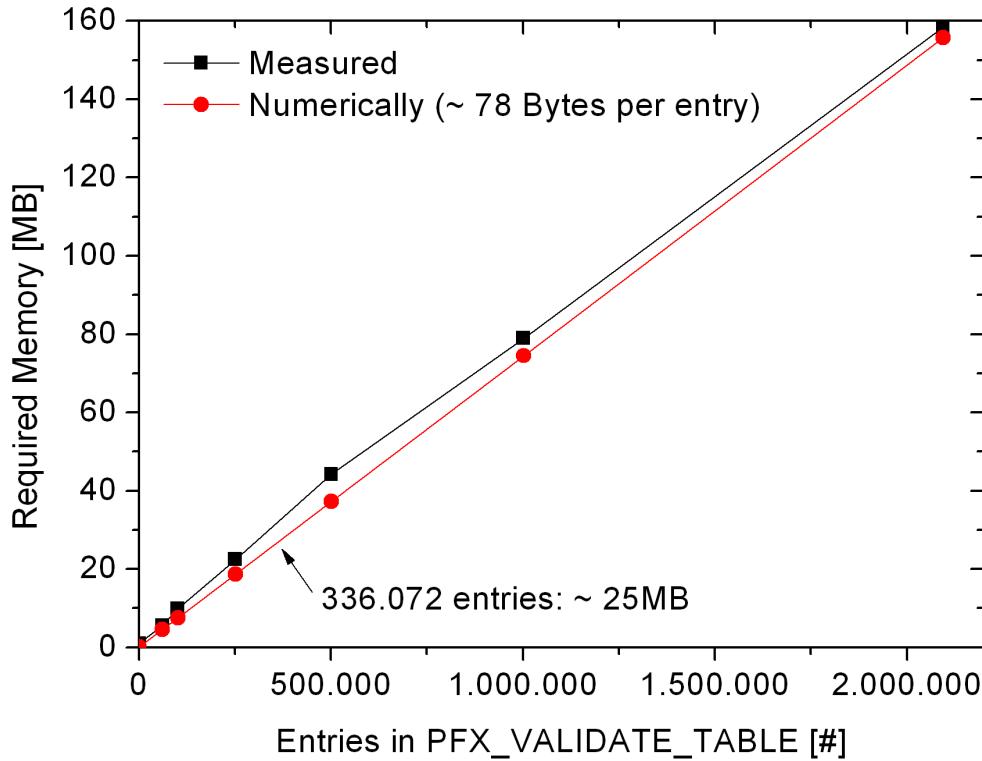
RPKI MIRO

- <http://rpki-miro.realmv6.org>
- <http://rpki-browser.realmv6.org>
- <https://github.com/rpki-miro>

Email: m.waehlisch@fu-berlin.de :: <http://www.inf.fu-berlin.de/~waehl>

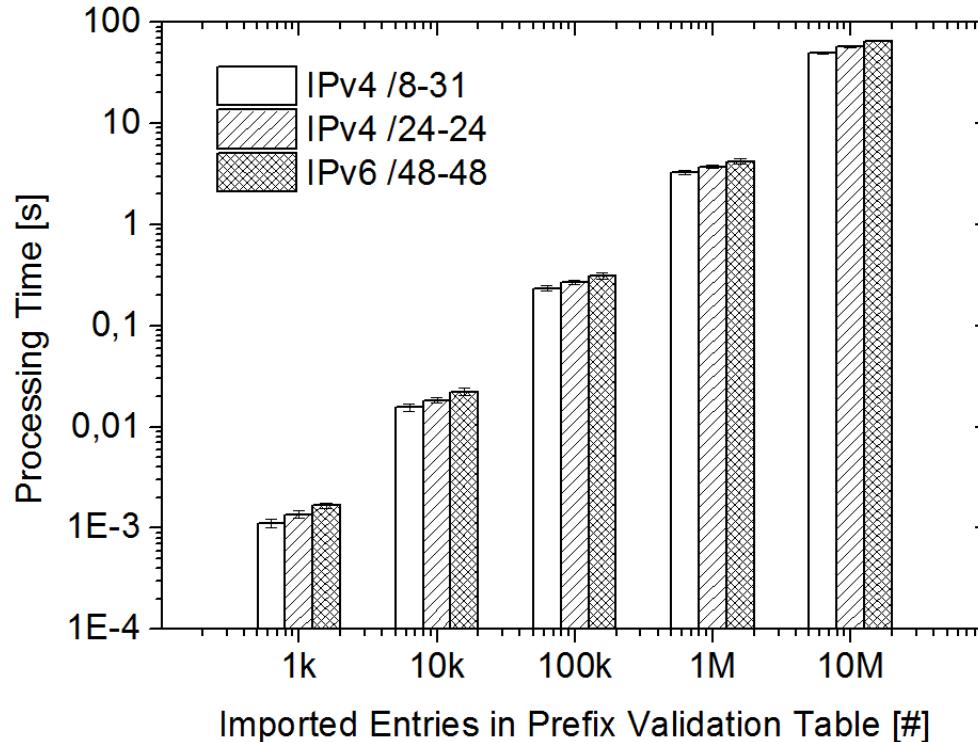
BACKUP

RTRlib: Memory Consumption



More details: M. Wählisch, F. Holler, T.C. Schmidt, J.H. Schiller, **RTRlib: An Open-Source Library in C for RPKI-based Prefix Origin Validation**,
In: Proc. of 7th USENIX Security Workshop on Cyber Security Experimentation and Test (CSET), Berkeley, CA, USA:USENIX Assoc., 2013.

RTRlib: Delay While Loading ROA Data



More details: M. Wählisch, F. Holler, T.C. Schmidt, J.H. Schiller, **RTRlib: An Open-Source Library in C for RPKI-based Prefix Origin Validation**,
In: Proc. of 7th USENIX Security Workshop on Cyber Security Experimentation and Test (CSET), Berkeley, CA, USA:USENIX Assoc., 2013.