

Cloudflare and RPKI at scale

Louis Poinsignon





Network Engineer at Cloudflare in San Francisco

Open-source projects including flows and RPKI

Network data collection (BGP, flows, peering-portal)



https://blog.cloudflare.com/rpki-details/ https://blog.cloudflare.com/rpki/

How did it start?





https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/



Authority DNS route hijack in April 2018.

This affected our DNS Resolver.

The route was sent to us on a Chicago peering session.

What should we do?



The Initial Story

At the time...

150+ PoPs, 26000 BGP sessions, IP space in 5 RIRs

Just the RIPE Validator^[1]

How to distribute a prefix list efficiently?



[1] Cloudflare is very grateful for the RIPE Validator s/w

The Initial Story

July: started deploying internally GoRTR.

August: open-source release. https://github.com/cloudflare/gortr

September \rightarrow December:

- Turn up RTR sessions
- Signing prefixes





Diagram





Behind the scene (until January 2019)

RIPE Validator providing list of prefixes.

Running in a Mesos cluster.

With a cronjob:

- Fetching the data
- Filtering it (remove > /24 and > /48 and duplicates)
- Signing it
- Making it available to our edge.

https://rpki.cloudflare.com/rpki.json was born.





Effects

The question everyone asked us.

How much traffic was affected?

Many invalids. Little traffic in practice (default or valid less specific).



https://www.flickr.com/photos/thure/6287816628/

Except in one place. Few gigabits per seconds displaced due to geographical more specific.



Accouting

Using flows, we see **at least <u>30%</u>** of the traffic being **valid**. Very **little/none invalid**.

We use **GoFlow** for accounting.

Other tools compatible with flows:

pmacct and Kentik





Signing the routes

Signing the routes

IP space in 5 RIRs (*no twnic/jpnic/cnnic*). Not a unified experience.

RIR	Features	Ease of use	ΑΡΙ
AFRINIC	*	*	*
APNIC	**	**	*
ARIN	**	**	**
LACNIC	*	***	*
RIPE	***	***	***





Features: RRDP, 2 factors, extra info, CA.

Ease of use: steps to sign a ROA, multi user.

API: functional, complete and accessible.



Comparison - AFRINIC

Hard to set up: client TLS certificate to create (BPKI) in order to do RPKI.

Buggy.

No RRDP.

No API.

No auto-renew.

Hosted CA possible.

Extensive certificate informations.





Comparison - APNIC

Two factors or client certificate. RRDP.

Auto-renew.

Allow BGP batch signing. (slight bugs with big amount of prefixes). Hosted CA possible.

Draft for API:

https://www.apnic.net/manage-ip/apnic-services/services-roadmap/public-api-draft-for-members/



Deuter	
eaister vour r	outes in MvAPNIC using the tool below. It will automatically create route of
uthorized. RP	KI ROAs will also be created at the same time, if the ROA option is enabled (
OA status wil	l not be updated until then).
nport rou	tes
GP announce	ments associated with your resources but not managed under this tool were
	hort from BCB Dismiss
Review & Im	DISINISS
Review & Imj	
Review & Imp	
Review & Imp	
Review & Imp Routes Create route	
Review & Imp Routes Create route Prefix	Route's prefix. E.g. 20310.0.0/20
Review & Imp Routes Create route Prefix Origin 45	Route's prefix. E.g. 203.10.0.0/20
Review & Imp Routes Greate route Prefix Origin AS	Route's prefix. E.g. 203.10.0.0/20 Route's origin. E.g. AS123
Review & Imp Routes Create route Prefix Origin AS Most specific	Route's prefix. E.g. 203.10.0.0/20 Route's origin. E.g. AS123 Route's most specific announcement. E.g. /22
Review & Im Routes Create route Prefix Origin AS Most specific announcement	Route's prefix. E.g. 203.10.0.0/20 Route's origin. E.g. AS123 Route's most specific announcement. E.g. /22
Review & Im Routes Preate route Prefix Origin AS Most specific announcement $oldsymbol{\Theta}$ ROA	Route's prefix, E.g. 203.10.0.0/20 Route's origin, E.g. AS123 Route's most specific announcement, E.g. /22 Image: Comparison of the system
Review & Im Routes Greate route Prefix Origin AS Most specific announcement ® ROA Whois	Route's prefix. E.g. 203.10.0.0/20 Route's origin. E.g. AS123 Route's most specific announcement. E.g. /22 Image: Comparison of the system
Review & Im Routes Create route Prefix Origin AS Most specific announcement O ROA Whois	Route's prefix. E.g. 203.10.0.0/20 Route's origin. E.g. AS123 Route's most specific announcement. E.g. /22 Image: Comparison of the state

Comparison - ARIN

Two factors. Separate signing key. No RRDP.

No auto-renew.

Semi-functional API (add).

Dashboard not easy to find.

Hosted CA possible.

Slow rsync update (4 times a day).

Some certificate information.

Create a Route	e Origin Authorization
Browser Signed	Signed
	* denotes required field
*ROA Na	me:
	Any name of your choosing.
*Origin	AS:
	The AS Number you are authorizing.
*Start Da	nte: 06-11-2018
	The first date your ROA can be considered valid.
*End Da	ate: 06-11-2028
	The last date your ROA can be considered valid.
*Prefix	Address CIDR Max Length
	O Add Prefix
	The prefixes you authorize to originate from this AS.
*Private K	Provide a Browse Browse
	This key will not be uploaded to ARIN.



Comparison - LACNIC

No two factors. Single user.

No RRDP.

No API.

Auto-renew opt-in.

Allow BGP batch signing.

Based off RIPE.

No Hosted CA.

Some extra info (revoked, path).

Incorrect certificate encoding (BER). High turnover of certificate (few days).



ASN
0
Valid until:
m 04/03/2021

Comparison - RIPE

Two factors.

RRDP.

Auto-renew.

Nice API.

Allow BGP batch signing.

No Hosted CA (theoretically).

No extra information. But history.

Incorrect certificate encoding (BER).

CLOUD	FLARE

E	3GP Announcements	Route Origin Auth	norisations (ROAs)	History	Search	
	C Discard Changes	逾 Delete ROAs	A Ca	using Problems	☑ Not Causing Problems	+ New ROA
	AS number	Prefix	Most allow	specific length red	Affects	
	AS Number	Prefix	Max	length		C 🖪

Automation

We automated prefixes adding on **ARIN and RIPE** with a **Salt state**.

Two secrets to store (API key and signing key).

Cannot delete or list via API for ARIN: very prone to mistakes if user wants to reduce the amount of ROA files.

```
def _format_payload(roas, signature):
    template = """----BEGIN ROA REOUEST-----
{roas}
----END ROA REQUEST----
----BEGIN SIGNATURE-----
{signature}
----END SIGNATURE-----
    ....
    payload = template.format(
        roas=roas, signature="n".join(textwrap.wrap(signature, width=64))
    return payload
def make roa(name, asn, t, start val, end val, prefix, length, maxlength):
    template = (
        '1|{time}|{name}|{asn}|{start val}|{end val}|{prefix}|{length}|{maxlength}|'
    time str = calendar.timeqm(t.timetuple())
    start val str = start val.strftime( TIME FORMAT)
    end val str = end val.strftime( TIME FORMAT)
    roa = template.format(
       time=time str,
       name=name,
       asn=asn,
       start val=start val str,
       end val=end val str,
       prefix=prefix,
       length=length,
       maxlength=maxlength,
    return roa
def sign(pkey, roas):
    signature = pkey.sign(roas.encode('utf-8'), padding.PKCS1v15(), hashes.SHA256())
    return base64.b64encode(signature).decode('utf-8')
```



Validator

Why making a validator?

First release of Routinator in November 2018. We were still using RIPE Validator.

We wanted something more custom: with monitoring and RRDP.

By building it in Go:

- Many APIs and easy for concurrency
- Community doing cryptography
- Cloudflare uses Go a lot (cfssl, sidh, etc.)





Juniper bugs: Routing Validation disabled.

Difficulties: rsync, BER encoded instead of DER, conditions in cryptography

3) a subjectPublicKeyInfo [<u>RFC5280</u>] in <u>DER</u> format [<u>X.509</u>], encoded in Base64 (see <u>Section 4 of [RFC4648]</u>). To avoid long lines, <<u>CRLF</u>> or <<u>LF</u>> line breaks MAY be inserted into the Base64-encoded string.

where the URI section is comprised of one of more of the ordered sequence of:



Cloudflare's RPKI Toolkit

Sets of libraries and tools written in Go.

Including OctoRPKI



https://blog.cloudflare.com/cloudflares-rpki-toolkit/

Cloudflare's RPKI Toolkit

Libraries

- CER/ROA/MFT decoder
- PKI manager (exploring, validating)
- RRDP/rsync fetcher
- Validation of prefixes





Cloudflare's RPKI Toolkit

Software

- Local validator (without RRDP/Rsync)
- API tools for a distributed version without filesystem
- OctoRPKI
- Certificate Transparency tool



OctoRPKI - Features (1/2)

- Decodes TAL/CER/ROA/MFT
- Explore via Manifest or directory.
- RRDP support (and failover to Rsync)
- Monitoring (Prometheus and JSON API which includes logs)
- Dockerizeable
- Handle stability (generate file when done)



OctoRPKI - Features (2/2)

- Full compatibility with GoRTR (including signing the JSON file)
- Server + caching options for generated file (CDN friendly)
- Configuration options
 - Disable/Enable components
 - Modes (server, one-off)
- ~5-15 minutes for a full cold-start sync



OctoRPKI - Compute footprint





avg

 rpki-benchmark-octorpki 	428 MB
- rpki-benchmark-ripe	906 MB
 rpki-benchmark-routinator 	511 MB

OctoRPKI v1.1.3 RIPE Validator v2.25 Routinator v3.3.0



Monitoring



75810

75800

8 min

<pre>NMF0[0002] Rsync sync rsync://rpki.ripe.net/rebsitory/arin-rpkit-dc.cer IMF0[0002] Rsync sync rsync://rpki.ripe.net/rebsitory/arin-rpki.cer IMF0[0004] Rsync sync rsync://rpki.ripe.net/rebsitory/lacnic/rta-lacnic-rpki.cer IMF0[0004] Rsync sync rsync://rpki.ripe.net/rebsitory/AfriMIX.cer IMF0[0004] Rsync sync rsync://rpki.afrinic.net/repository/4E880080F4D11E08657D8931367AE7D/62gPOPXWxxu0sQa4vQ2YUBLaWb Y_mft: no such file or directory EGNN [0012] Error exploring file: open cache/rpki.arin.net/repository/asB08214166511E2B3BC286172FD1F72/C5zKkW0keoo3ZmsZIX_g2EA3t6I. mft: no such file or directory EGNN [0012] Error exploring file: open cache/rpki.arin.net/repository/ipe-ncc-ta.mft: no such file or directory EGNN [0012] Error exploring file: open cache/rpki.rep.net/rpki/lacnic/rta-lacnic-rpki.mft: no such file or directory IMF0[0012] Still exploring. Revalidating now IMF0[0012] SRDP sync https://rrdp.apnic.net/notification.xml INF0[00012] RRDP sync https://rrdp.apnic.net/notification.xml INF0[00064] RRDP: https://rrdp.ripe.net/notification.xml INF0[00664] RRDP showshot.xml Downloading snapshot at: https://rrdp.ripe.net/Asb7553b-b124-4717-b20c-105a </pre>	0.0.0	1. docker		• • •	127.0.0.1:8080/infos	x 1 127.0.0 1:8080/output isor	x +	
<pre>INFO[0002] Rsync sync:rypk:/rpki.afrinic.net/repository/lacnic/rta-lacnic-rpki.cer INFO[0007] Rsync sync:rsync://rpki.afrinic.net/repository/AfriNIC.cer INFO[0007] Rsync sync:rsync://rpki.afrinic.net/repository/AfriNIC.cer INFO[0007] Error exploring file: open cache/rpki.afrinic.net/repository/04E880D80F4D11E08657D8931367AE7D/62gPOPXWxxu0sQa4vQZYUBLaMb // "file=control i, " ifile=control i, " ifile=contr</pre>	INFO[0002] Rsync sync rsync://rpki.arin.net/repository/ari	n-rpki-ta.cer			@ 4070 04:0000 5-4-			
<pre>INFO[0004] Rksync Sync: Type://repsitory.tachtc.net/rpki.cer", "irr:": "type://rpki.afrinic.net/rpsitory/AttNIC.cer", "irr:": "type://rpki.afrinic.net/rpsitory/4E880080F4D11E08657D8931367AE7D/62gP0PXWxxu0sQa4vQZYUBLaMb Y.mft: no such file or directory ERRO[0012] Error exploring file: open cache/rpki.apric.net/repository/A166511E283BC286172FD1FF2/C5zKkN0Neoo3ZmsZIX_g2EA3t6I. Thft: no such file or directory ERRO[0012] Error exploring file: open cache/rpki.arin.net/repository/a1anic.ret/rpki/lacnic/rta-lacnic-rpki.mft: no such file or directory ERRO[0012] Error exploring file: open cache/rpki.arin.net/repository//aianic/rta-lacnic-rpki.mft: no such file or directory ERRO[0012] Error exploring file: open cache/rpki.iripe.net/rpki/lacnic/rta-lacnic-rpki.mft: no such file or directory ERRO[0012] Error exploring. Revalidating now INFO[0012] Still exploring. Revalidating now INFO[0012] RRDP: Downloading ront ontification.xml INFO[0012] RRDP: Downloading ront ontotification.xml INFO[0046] RRDP: https://rrdp.apnic.net/notification.xml INFO[0064] RRDP: Nttps://rrdp.ripe.net/notification.xml INFO[0064] RRDP: Nttps://redp.ripe.net/notif</pre>	INFO[0002] RSync Sync rsync://rpki.ripe.net/ta/ripe-ncc-ta	.cer	4	⇒ G	0 127.0.0.1:8080/into	S		¥ 0 :
<pre>INFO[0007] KSpNL SpNL rspNL://rpkl.utrintc.net/repository/4E880080F4D11E0865708931367AE7D/62gP0PXWxxu0sQa4vQZYUBLaMb Y.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.arin.net/repository/48880B214166511E2B3BC286172FD1FF2/C5zKkN0Neoo3ZmsZIX_g2EA3t6I. FRR0[0012] Error exploring file: open cache/rpki.arin.net/repository/arin-rpki-ta.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.arin.net/repository/arin-rpki-ta.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.arin.net/repository/arin-rpki-ta.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.ripe.net/repository/ipe-ncc-ta.mft: no such file or directory ERR0[0012] Still exploring. Revalidating now INF0[0012] RRDP sync https://rrdp.apnic.net/notification.xml INF0[0012] RRDP sync https://rrdp.apnic.net/notification.xml Downloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1 INF0[0064] RRDP sync https://rrdp.ripe.net/notification.xml INF0[0064] RRDP sync https://rrdp.ripe.net/noti</pre>	INFO[0004] RSync Sync rsync://repository.idenic.net/rpki/L	achic/rta-lachic-rpki.cer			"uri": "rsync://repo	sitory.lacnic.net/rpki/lacnic/	rta-lacnic-rpki.cer",	
<pre>Environment = = = = = = = = = = = = = = = = = = =</pre>	[DD0[001] Rsync sync rsync://rpki.drrintc.net/repository/		alth		"file-count": 1, "iteration": 1.			
<pre>T.mtc. No Such Tite of Alrectory ERRO[0012] Error exploring file: open cache/rpki.apic.net/repository/8380B214166511E2B3BC286172FD1FF2/C5zKkN0Neoo3ZmsZIX_g2EA3t6I. mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.arin.net/repository/arin-rpki-ta/arin-rpki-ta.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.ripe.net/repository/lacnic/rta-lacnic-rpki.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.ripe.net/repository/lacnic/rta-lacnic-rpki.mft: no such file or directory ERR0[0012] Error exploring file: open cache/rpki.ripe.net/repository/ripe-ncc-ta.mft: no such file or directory INF0[0012] Still exploring. Revalidating now INF0[0012] RRDP sync https://rrdp.apnic.net/notification.xml INF0[0012] RRDP: bownloading root notification https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1 233b30f503/83968/snapshot.xml INF0[0064] RRDP: sync https://rrdp.ripe.net/notification.xml INF0[0064] RRDP: sync https://rrdp.ripe.net/notification.xml INF0[0064] RRDP: https://rrdp.ripe.net/notification.xml</pre>	KRO[0012] Error exploring file: open cache/rpki.arrinic.n	ες, μεροχιτοιλιατεφραρφοιτητεαρος, παρχτροι με τη ος βληλιματάργατη το το	amb		"errors": 0,			
<pre>text [0012] Error exploring Tite: open tucher/pixt.dpmt.the/repository/ssbb2i+tb0511t255bc2a07rPDFP2C52ktkWebe052m521A_g22E45t01.</pre>	EPPOEOA12] Empon evaloring file: open cache (mpki annic net	/managatamy//82800211166511520200286172501552/(57K)/MANaga27mc7TV_a2543+	GT		"duration": 2.961329	6, 2002		
<pre>mint the of united of united of united of y ended of the provided of the</pre>	mft: no such file on directory	/ repusit cory/ 8380621410031162636C2801/2r01rr2/C32KKWWWe0032m521A_92EA30	01.	},				
<pre>END_001_] Error exploring file: open cache/repository.lacinc.net/rpkit cus in pkt cus in the or directory ERR0[0012] Error exploring file: open cache/repository.lacinc.net/rpkit.imft: no such file or directory INF0[0012] Error exploring file: open cache/repository.lacinc.net/rpkit.imft: no such file or directory INF0[0012] Error exploring file: open cache/repository.lacinc.net/rpkit.imft: no such file or directory INF0[0012] Error exploring file: open cache/repository.lacinc.net/rpkit.imft: no such file or directory INF0[0012] Revolidating now INF0[0012] RRDP: Downloading root notification.xml INF0[0012] RRDP: Downloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1 INF0[0064] RRDP sync https://rrdp.rpie.net/notification.xml INF0[0064] RRDP sync https://rrdp.ripe.net/notification.xml INF0[0064] RRDP sync https:/</pre>	ERRO[0012] Error exploring file: open cache/rpki arin net/	renository/arin-rnki-ta/arin-rnki-ta mft: no such file or directory		× ("uri": "rsvnc://rpki	.afrinic.net/repository/AfriNI	C.cer".	
<pre>BRAID [0012] Error exploring file: open cache/rpki.ripe.net/repository/ripe-ncc-ta.mft: no such file or directory INFO[0012] Error exploring, Revalidating now INFO[0012] RRDP sync https://rrdp.apnic.net/notification.xml INFO[0012] RRDP: https://rrdp.apnic.net/notification.xml UNFO[0012] RRDP sync https://rrdp.apnic.net/notification.xml UNFO[004] RRDP sync https://rrdp.ripe.net/notification.xml INFO[004] RRDP sync https://rrdp.ripe.net/notification.xml INFO[004] RRDP sync https://rrdp.ripe.net/notification.xml INFO[004] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0046] RRDP: https://rrdp.ripe.net/notification.xml INFO[0046] RRDP: https://rrdp.ripe.net/notification.xml INFO[0046] RRDP: https://rrdp.ripe.net/notification.xml</pre>	ERRO[0012] Error exploring file: open cache/renository lac	nic net/rnki/lacnic/rta-lacnic-rnki mft: no such file or directory			"file-count": 1,			
<pre>INFO[0012] Still exploring. Revalidating now INFO[0012] RRDP sync https://rrdp.apnic.net/notification.xml INFO[0012] RRDP: https://rrdp.apnic.net/notification.xml INFO[0014] RRDP: https://rrdp.apnic.net/notification.xml INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RDP: https://rrdp.rip</pre>	ERRO[0012] Error exploring file: open cache/reki rine net/	repository/rine-ncc-ta mft: no such file or directory			"iteration": 1, "errors": 0.			
<pre>INFO[0012] RRDP Sync https://rrdp.apnic.net/notification.xml INFO[0012] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml INFO[0014] RRDP: https://rrdp.apnic.net/notification.xml INFO[0044] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml</pre>	INFO[0012] Still exploring. Revalidating now				"duration": 4.390532	3,		
<pre>INFO[0012] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml INFO[0012] RRDP: https://rrdp.apnic.net/notification.xml Downloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1 233b30f503/83968/snapshot.xml INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: Downloading root notification https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml</pre>	INFO[0012] RRDP sync https://rrdp.apnic.net/notification.x	ml		>	"last-fetch": 155034	2006		
<pre>INF0[0014] RRDP: https://rrdp.apnic.net/notification.xml Downloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9-b1 233b30f503/83968/snapshot.xml INF0[0064] RRDP sync https://rrdp.ripe.net/notification.xml INF0[0064] RRDP: bownloading root notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a INF0[0064] RRDP: https://rrdp.ripe.net/notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a</pre>	<pre>INFO[0012] RRDP: Downloading root notification https://rrd</pre>	p.apnic.net/notification.xml		1.				
233b30f503/83968/snapshot.xml INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: Downloading root notification https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml	<pre>INFO[0014] RRDP: https://rrdp.apnic.net/notification.xml D</pre>	ownloading snapshot at: https://rrdp.apnic.net/fa64523b-7381-4fda-9eb9	-b1	v "sias-r	rdp": [
INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: Downloading root notification https://rrdp.ripe.net/notification.xml INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a	233b30f503/83968/snapshot.xml				"uri": "https://rrdp	.apnic.net/notification.xml",		
INF0[0064] RRDP: Downloading root notification https://rrdp.ripe.net/notification.xml INF0[0064] RRDP: https://rrdp.ripe.net/notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a	<pre>INFO[0064] RRDP sync https://rrdp.ripe.net/notification.xm</pre>	1			"file-count": 6734, "iteration": 1,			
INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml Downloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-105a	<pre>INFO[0064] RRDP: Downloading root notification https://rrd</pre>	p.ripe.net/notification.xml	1919		"errors": 0,			
	<pre>INFO[0064] RRDP: https://rrdp.ripe.net/notification.xml Do</pre>	wnloading snapshot at: https://rrdp.ripe.net/8ab7553b-b124-4717-b20c-10	05a		"duration": 52.05189 "last-fetch": 155034	39, 20590.		
da07476c/866/snapshot.xml	da07476c/866/snapshot.xml				"rrdp-serial": 83968	, ,		
INFO[0177] Rsync sync rsync://repository.lacnic.net/rpki/lacnic	INFO[0177] Rsync sync rsync://repository.lacnic.net/rpki/l	acnic			"rrdp-sessionid": "for "rrdp-last-file": "h	a64523b-7381-4fda-9eb9-b1233b3 ttps://rrdp.apnic.net/fa64523b	0f503", -7381-4fda-9eb9-	
INFO[0241] Rsync sync: rsync://rpki.arin.net/repository	<pre>INFO[0241] Rsync sync rsync://rpki.arin.net/repository</pre>		Ale -		b1233b30f503/83968/s	napshot.xml"		
INFO[0298] Rsync sync: rsync://rpki.afrinic.net/repository	<pre>INFO[0298] Rsync sync rsync://rpki.afrinic.net/repository</pre>			}, 				
INFO[0309] Rsync sync rsync://rpki.apnic.net/repository	INFO[0309] Rsync sync rsync://rpki.apnic.net/repository		1. and the		"uri			
			30	Al same		ΔΡΙ		S. A. Martine

\$ []

Validator

2....

1. docker		
INFO[0842] RRDP sync https://rrdp.apnic.net/notification.xml	● ● ● □ 127.0.0.1:8080/infos × □ 127.0.0.1:8080/output.json × □ 127.0.0.1:8080/metri	cs × +
INFO[0842] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml	← → C ① 127.0.0.1:8080/output.json	☆ 0 :
INFO[0844] RRDP: https://rrdp.apnic.net/notification.xml has 0 deltas to parse (cur: 83980, last: 83980)	/"matadata",	
INFO[0844] RRDP: finished downloading https://rrdp.apnic.net/notification.xml. Last serial 83981	{"counts":76058, "generated":1550343058, "valid":1550346658, "signature": "3045022100b5d	b8f44bdab78b418d
INFO[0844] RRDP sync https://rrdp.apnic.net/notification.xml	6ef5ec55f687794ed723c63c63cfe705fbe65ba10db1002202a7b6eaec89bb8bd845b481f7aa20ebf2fd 95429fe39c82e", "signatureDate":"3045022100f0368e9cdf510c55ae28387a87fbdc415636f97c86	2a0df54b81bcf709 fbe5af065c29514c
INFO[0844] RRDP: Downloading root notification https://rrdp.apnic.net/notification.xml	f77e8c02202fcfd496a9b2c166b9e4c7cb2fb410ecad406f1c03d05024dce2ee71b9177de5"}, "roas":	
INFO[0845] RRDP: https://rrdp.appic.net/notification.xml has -1 deltas to parse (cur: 83980, last: 83981)	{"prefix": "91.204.44.0/22", "maxLength": 32, "asn": "AS197540", "ta": ""},	
TNEO[0845] RRDP: finished downloading https://rrdp.appic.net/notification.xml. last serial 83981	{ "prefix": "190.108.216.0/22", "maxLength": 24, "asn": "AS265751", "ta": ""}, { "prefix": "186.179.112.0/20", "maxLength": 24, "asn": "AS27755", "ta": ""},	
THEOREMS I REDE SALE HERS //rede rise pet/actification xml	<pre>{"prefix":"190.2.224.0/20", "maxLength":24, "asn":"AS27755", "ta":""},</pre>	
THEOREASI REPORT Downloading root notification https://mrdg.rine.net/notification.xml	{"prefix":"172.69.84.0/22", "maxLength":22, "asn": "AS13335", "ta":"},	
THEORES I RED: between the net (notification will has a 1 datas to naree (cur. 867 last: 868)	{"prefix":"77.74.76.0/24","maxLength":24,"asn":"AS206850","ta":""}, {"prefix":"37.130.198.0/24","maxLength":24,"asn":"AS199386","ta":""},	
THEORES REDUCTION TO A CONTRACT AND	{"prefix":"37.130.199.0/24", "maxLength":24, "asn":"AS199386", "ta":""}, {"prefix":"37.130.196.0/24", "maxLength":24, "asn":"AS199386", "ta":""},	
THEOREGIS PROP. HTTESTICE USING USING USING THE STATE OF	{"prefix":"37.130.197.0/24", "maxLength":24, "asn": "AS199386", "ta":""},	
INCOLOGY (NOT Sync Incos, // percentice.cl// Hup/hoter). And	{ "prefix": "2a04:dc0::/32", "maxLength":32, "asn": "AS199386", "ta": "}, { "prefix": "2a04:dc1::/32", "maxLength":32, "asn": "AS199386", "ta": ""},	
THEO[095] NOT: Downloading foot not intertation integs://ipt.tonnet.cn/rtg/notify.xmt	{"prefix":"220.216.104.0/23", "maxLength":24, "asn":"AS10010", "ta":""}, {"prefix":"185.132.68.0/22", "maxLength":22, "asn":"AS203489", "+=".""]	
THEORON' INCOV. Inclus. The content of the provided and t	{"prefix":"185.214.0.0/22", "maxLength":22, "asn":"AS203489", "ta":"},	
Thro[0647] Nor. Finished downtodding https://rpki.chntc.ch/rrap/hottry.xml. Last serial 255275	<pre>{ pre1x :- zaub:91c0::/29", "maxLength":29, "asn": "A5203489", "ta":"" },</pre>	
INFO[0647] RSynC SynC://pkt.artn.net/repository	{"prefix":"192.188.53.0/24","maxLength":24,"asn":"AS23487","ta":""}, {"prefix":"122.129.82.0/24","maxLength":24,"asn":"AS38264","ta":""},	
INFO[0801] KSynC SynC rSynC://pkt.afrinic.net/repository	{"prefix":"122.129.83.0/24", "maxLength":24, "asn": "AS38264", "ta":""},	
INFO[086/] RSync Sync rsync://pki.ripe.net/ta/ripe-ncc-ta.cer	{"prefix":"203.128.15.0/24", "maxLength":24, "ash":"AS38264", "ta":""}, {"prefix":"203.128.16.0/24", "maxLength":24, "ash":"AS38264", "ta":""},	
INFO[0869] RSync Sync rSync://repository.lacnic.net/rpki/lacnic	<pre>{"prefix":"2600:9000:1044::/48","maxLength":48,"asn":"AS16509","ta":""}, {"prefix":"104.28,176.0/20","maxLength":20,"asn":"AS13335","ta":""},</pre>	
INFO[0883] Rsync sync rsync://rpki-repository.nic.ad.jp/ap/A91A73810000	{"prefix":"185.154.130.0/24","maxLength":24,"asn":"AS58059","ta":""},	
INFO[0885] Rsync sync rsync://rpkica.twnic.tw/rpki/TWNICCA	{"prefix":"185.154.128.0/24","maxLength":24,"asn":"AS58059","ta":""}, {"prefix":"185.154.131.0/24","maxLength":24,"asn":"AS58059","ta":""},	
MARN[10]] Resource kk71cA20,W146-RadEKAYKh17kkespt is invalid: <nil></nil>	{"prefix":"185.154.129.0/24","maxLength":24,"asn":"AS58059","ta":""}, {"prefix":"185.252.128.0/22","maxLength":22.	
_NFO[1065] Stable state. Revalidating in 20m0s	{"prefix":"185.252.129.0/24","maxLength":24	
	ROA list	10.20
	I CONTISC	23 S-14
	"counts": 76058,	
	generatea : 1550343058, "valid": 1550346658	
	"si anature": "3045022100b5db8f44bdab78b418d6ef6ec55f687794ed72	3c63c63cfe705fh
	e65ba10db1002202a7b6eaec89bb8bd845b481f7aa20ebf2fd2a0df54b81bcf709	95429fe39c82e".
	"signatureDate": "3045022100f0368e9cdf510c55ae28387a87fbdc4156	36f97c86fbe5af0
	65c29514cf77e8c02202fcfd496a9b2c166b9e4c7cb2fb410ecad406f1c03d0502	4dce2ee71b9177d
	e5"	
	},	
	"roas": L	
	"prefix": "216.59.62.0/24".	
	"maxLenath": 24.	
	"asn": "AS36167",	
	"ta": ""	
	},	
	{	
	"nrefix" "91 704 44 0/22"	
	s cat output.json/ jq '.roas / length'	
	10000	

OctoRPKI - Run it yourself



GoRTR

OctoRPKI does not embed a RTR server. Modular and independence! Fully compatible with **GoRTR** <u>https://github.com/cloudflare/gortr</u> Signs the prefix list to ensure a safe distribution of the file.

Can run natively on Juniper!

\$ docker run -ti \
-p 8082:8082 \
<pre>-v \$PWD/example.pub:/example.pub \</pre>
cloudflare/gortr \
-verify.key /example.pub \
-cache https://YOUR_ROA_URL





Only software to support **plaintext**, **SSH** and **TLS**.

Compatibility matrix

A simple comparison between software and devices. Implementations on versions may vary.

Device/software	Plaintext	TLS	SSH	Notes
RTRdump	Yes	Yes	Yes	
Juniper	Yes	No	No	
Cisco	Yes	No	Yes	Only SSH password
Alcatel	Yes	No	No	
Arista	No	No	No	
FRRouting	Yes	No	Yes	Only SSH password
Bird	Yes	No	Yes	Only SSH key
Quagga	Yes	No	No	



GoRTR without installing anything

SSH: rtr.rpki.cloudflare.com:8283 (user: rpki/pass: rpki)

and

Plaintext: rtr.rpki.cloudflare.com:8282

Just configure your router



Cloudflare's Internal Version

Is providing: https://rpki.cloudflare.com/rpki.json

But also a GraphQL API

...which powers a **dashboard**

• guery(resource(an:13335) { { { { { { (untot of the set of the	
<pre>abjects:id= abjects:id= vviid?open strid strid prome on Certificate(</pre>	Q. Search resource No Description Fits.00 subjectKeyKd: String authorityKd: String authorityKd: String path: String path: String market: String market: String contracts Market: Cartificate ROA



Dashboard

				← → C ■ https://staging.rpki.cloudflare.com/?keyid=&prefix=1.1.1.0%2F32 ☆ ① III Apps _ SVG Crowbar □ Other Box								
\rightarrow C \Rightarrow https://staging.rpki.cloudflare.com/?ta=				CLOUDFLARE RPKI Dashboard								
RPKI Dashboard							TRUST ANCHOR:	KEY ID:	PREFIX:	ASN: Enter an AS number		
TRUST ANCHOR: KEY ID:			Resource List Hierarchical View			Address Space View						
Resource List	e List Hierarchical View				Found 2 ROAs and 9 certificates ROAs							
nowing 5 certificates and 0 ROAs				ASN	Prefix	Max Length	IP Family	Trust Anchor	Emitted	Expiration		
ertificates				AS13335	1.0.0.0/24	/24	IPv4	APNIC	3/16/2018	in 2 years		
Кеу	Name	Trust Anchor	ASNs									
e8552b1fd6d1a4f7e404c6d8e5680d1ebc163fc 3	ripe-ncc-ta	RIPE	0- 429496	Name: Saab/815-9744								
fc8a9cb3ed184e17d30eea1e0fa7615ce4b1af47	root trust anchor O=lacni c	LACNIC	0- 429496	Trust Anchor: APNIC Key: as24090e86c3bc39ee7ac345b3bf9a38cd9ff3ad Parent Key: 68faf9dace19768cac3d4ed7bb24372bffa6d018 Path: rsync:/rtpki.apnic.net/member_repository/A91872ED/ED8C96901D6C11E28A38A3AD08B02CD2/797B4DEC293 B11E88187196DC4F9AE02.roa Validity: Fri, 16 Mar 2018 17:00:05 GMT - Wed, 31 Mar 2021 00:00:00 GMT								
0b9cca90dd0d7a8a37666b19217fe0d84037b7 a2	apnic-rpki-root-iana-origi n	APNIC	1- 429496									
eb680f38f5d6c71bb4b106b8bd06585012da31 b6	AfriNIC-Root-Certificate	Afrinic	0- 429496	Emitted: Fri, 16 Mar 2018 17:00:05 GMT ASN: 13335 Prefix: 1.0.0.0/24								
				Max Length: //	24							



Certificate Transparency

Historical records of certificates.

Contains a chain (root \rightarrow ROA).

Sent by our validator.





Other data - so how fresh are those ROAs?



Future projects or ideas

RPKI validation tester using our CDN:

• Using a /23 (/47 IPv4) valid and a /24 (/48 IPv6) invalid

Certificate encoder, ASPA.

More toolings and visualizations around RPKI (BGP collection):

• Integration in our portal <u>peering.cloudflare.com</u> (ask for your free access)



Recent Leaks And Conclusions

Summary of Amazon Route Hijack

An attacker announces Amazon Authority DNS prefixes.

Cloudflare and Google accept them in specific locations.

Cloudflare and Google DNS resolvers use this route when clients request the website, the attacker's server is returned.

The server has a phishing website for the client.

Attacker gather credentials and steals Bitcoins.











Summary of Amazon Route Hijack

Amazon did not have signed routes.

Cloudflare did not do RPKI validation + route filtering

If RPKI was deployed:

Route would have been rejected because wrong origin.



Summary of Verizon Route Leak

A company has two Internet accesses: Verizon and another ISP.

The ISP has a BGP optimizer which feeds more-specific routes.

Unfortunately, the ISP sends the routes to the company which end up being sent to Verizon.

Verizon did not filter them and re-announces them to its peers and clients.







Summary of Verizon Route leak

Cloudflare had signed routes.

Verizon did not filter. Many networks accepted the leak.

Cloudflare filtering routes did not matter here.

If basic filtering was deployed:

Peering sessions would have been removed when going above prefix threshold. AS-Path filtering could have avoided accepting routes.

If RPKI was deployed:

Routes would have been rejected because wrong length.



What we learned

RPKI will not be the solution to everything. But in our stories...

Filtering solves Amazon being hijacked

Signing helps your network not being leaked



Deploy RPKI now

Because tomorrow is already too late

Traffic Volume AS7018 - AT8 With	n filtering	Qu	lume AS701 - Verizon	With	out fi	Itering	Query Time:
Overview Traffic Typ All Amsterdam, NL Houston, US Zurch, CH (ofher)	Bandwidth Graphs De: Traffic Direction: Location: From Cloudfi All Atlanta, US Buffalo, US Chennal, IN Chicago, US Miami, US	PoPs Breakdown per: Met Location Bil allas, US Denver, US allas, US St. Louis, US	Amsterdam, NL Dublin, IE Tampa, US	Traffic Type: All All Alanta, US Los Angeles, US (other)	Traffic Direction: Ucatie From Cloudfl V All Boston, US Buffalo, U Montgomery, US Montréal, 2A	on: Breakdown per: Location Charlotte, US Chicago, US Da Newark, US Norfolk, US Sa	Metric: Bits las, US Detroit, US Seattle, US
Gbs							
02:45 06 PM 09 PM	Mon 24 03 AM 06 AM Time (local)	09 AM 12 F	1 5 06 PM	09 PM M	on 24 03 AM Time (local)	06 AM 09 AM	12 PM 02:45



Thank you

Questions?

louis@cloudflare.com @lpoinsig (twitter)



