

### **Developments in Routing** Security and RPKI



Oleg Muravskiy

23 September 2022 | RIPE NCC Days Tashkent

### **RIPE NCC – Who We Are**

- the Middle East and parts of Central Asia
  - Ensure unique holdership •
  - Document holdership in the RIPE Database (whois) •
  - Issue digital certificates for allocated IP resources
  - •

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022 |





# • We manage ASN and IP address allocations in Europe,

# Enable operators to document use of their address space

### **Routing Security Is in Our DNA**

- In 1993, RIPE-81 was the first document published that used a common language to describe routing policies
- We co-developed standards for the Internet Routing Registry (IRR) and Resource Public Key Infrastructure (RPKI)
- We are one of the five RPKI Trust Anchors



## Internet Routing (In)Security



### Routing on the Internet (BGP)

Net A 10.10.x.x

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022





Net B 10.20.x.x

### Routing on the Internet (BGP)









### Routing on the Internet (BGP)





### Incidents Are Common

### • <u>2017 Routing Security Review</u> by the Internet Society

- 14k incidents
- 10% of all ASes affected
  - 3k ASNs were victims of at least one incident
  - 1.5k ASNs caused at least one incident
- BGP Security in 2021 by the Internet Society
  - 775 possible hijacks + 830 BGP leaks



### Incidents in 2022

- A misconfiguration on Mikrotik routers looked like a hijack from single-digit ASNs
- 26 July <u>Rostelecom hijacked Apple</u> for 12 hours
- 28 March <u>RTComm hijacked Twitter</u>



### Non-Incidents Also Became Common

- BGP and DNS hijack targeting Amazon and MyEtherWallet.com (April 2018)
- BGP hijack of Amazon space attacking users of Celer Network (August 2022)





### How to Secure Routing?





### **Resource Public Key Infrastructure (RPKI)**

- RIRs issue digital certificates (X.509) to IP and ASN holders
- Certificate holders can cryptographically sign (routingrelated) statements, for example:
  - AS X is authorised to announce my IP prefix Y
  - Signed by the holder of Y
- RPKI repositories operated by all RIRs since 2011
- IETF works on standards



### **RPKI Route Origin Validation (ROV)**









# Creating validation records



### Creating RPKI Objects: Running Your Own CA

- Install RPKI CA software
  - Dragon Research Labs rpki.net RPKI toolkit
  - NLnet Labs Krill
- Enable non-hosted CA on LIR Portal
- Set up connection with RIPE NCC CA
- Generate your resource certificate and get it signed
- Create your ROA objects
- Publish your resource certificate and ROA objects in your RPKI repository
- Keep re-publishing your objects (every 24 hours) (from another AS)



### **Creating RPKI Objects: Using Hosted CA**

- Install RPKI CA software
  - Dragon Research Labs rpki.net RPKI toolkit
  - NLnet Labs Krill
- Enable non-hosted CA on LIR Portal
- Set up connection with RIPE NCC CA
- Generate your resource certificate and get it signed
- **Create your ROA objects**
- Publish your resource certificate and ROA objects in your RPKI



### Enable Hosted CA on the LIR Portal



ie LIR Portai	
RIPE Database (Whois) Website   Search the content of this website	Q
e > Get Support > Publications > About Us	>
You are editing	٣
Ate the Terms and Conditions for the RIPE NCC Certification Service. The RIPE NCC sed on Internet Engineering Task Force (IETF) standards, in particular RFC3647, "Internet cture Certificate Policy and Certification Practices Framework", RFC3779, "X.509 es and AS Identifiers", and the "Certificate Policy (CP) for the Resource PKI (RPKI)". ONS ons, the following terms shall be understood to have the meanings assigned to them rity	
s and Conditions.	
onvice Announcements   Drivery Statement   Legal   Cookies   Conveight Statement   Term of Servi	



### Create Your ROA Objects in a Hosted CA

Manage IPs and ASNs >	Analyse	e > Partic	cipate >	Get Support	> Pub	lications >	About Us >
You are here: Home > Manage IPs an	id ASNs > LIR	R Portal			You ar	e editing	Ψ
My Account	>	RPKI Dashboard			36 CERTIFIED	RESOURCES NO ALE	RT EMAIL CONFIGURED
Resources My Resources Sponsored Resources Request Resources	~	SBGP And Valid	<b>າວບກວອກ</b> nvalid ? ເ	<b>J</b> nknown	ERC CK	DAS Causing pre-	oblems
Request Transfer IPv4 Transfer Listing Service RPKI Dashboard RIPE Database	>	<b>BGP Announcements</b> There are currently no l	Route Origin A	Authorisations (ROAs	As) History Causing Problems	Search	ns + New ROA
		AS number	Prefix	Mo allo	ost specific length owed	Affects	
		AS Number	Prefix	Ma	ax length		C 🖪
		Show 25 \$ of 0 items					
Muravskiy   RIPE NCC Days Tashke	ent   23 Ser	otember 2022			https://you	tu.be/gLwHp12	2wOGw



### Create Your ROA Objects in a Hosted CA

Manage IPs and ASNs >	Analyse	> Participa	ate >	Get Support	> Publication	s >	Ab	out Us
You are here: Home > Manage IPs and ASNs > LIR Portal					You are editing			
My Account	🕸 RPKI Dash	board			9 CERTIFIED RESOUR	CES	NO ALERT EMA	
Resources	न्द <b>41</b> ।	RGP Annoi	inceme	nts				
My Resources			incente	h				
Sponsored Resources	🧧 <b>4</b> Valid	! 1 Invalid	? 36 Un	known	<b>3</b> OK	1 Causi	ng problem	าร
Request Resources								
Request Transfer	BGP Announcer	nents Route Origin A	uthorisations (RO	As) History	Sear	ch		
IPv4 Transfer Listing Service								
RPKI Dashboard	Create R	OAs for selected BGP Ann	ouncements			🗹 Valid	A Invalid	O Unknown
RIPE Database	Origin AS	Pref	ix	Current Status				
	AS12654	2001	:7fb:fe01::/48	UNKNOWN				V.S. P.
	AS12654	2001	:7fb:fe0c::/48	UNKNOWN				V.S. V
	AS12654	2001	:7fb:fe0f::/48	UNKNOWN				V.S. V.
	AS12654	2001	:7fb:ff00::/48	UNKNOWN				
	AS12654	2001	:7fb:ff01::/48	UNKNOWN				12 V
	A\$12654	200	•7fb•ff02••/49					C. H



### **Creating RPKI Objects: Using Hosted CA**

- Enable Hosted CA in the LIR Portal
- Create your ROA objects
- We will publish your objects in our RPKI repository
- We will keep your objects up to date

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022 |



45 seconds (if you know your **RIPE NCC Access** password)

### Hosted CA for PI End Users

- By default, RPKI for PI resources is managed by the sponsoring LIR
- that maintainer
- ...and enable your own RPKI CA
- **Documentation**

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022





### Your sponsoring LIR could make you the maintainer of an inetnum object for your resources in the RIPE DB

### Then you could link your RIPE NCC Access account to

# Validating received routes



### Validating Route Announcements



Oleg Muravskiy RIPE NCC Days Tashkent 23 September 2022



Your peer



BGP

### **RPKI-to-Router**



### Your router

### Validating Route Announcements





### Validating Route Announcements: Policies

- Prefer VALID over others
- Prefer NOT FOUND over INVALID
- Reject INVALID?
  - "There are too many of them!"

Oleg Muravskiy RIPE NCC Days Tashkent 23 September 2022



### Invalid == reject ?

- What breaks if you reject invalids?
  - "Mostly nothing" AT&T
  - "5 customer calls in 6 months, all resolved quickly" medium Dutch ISP
  - "Customers appreciate a provider who takes security seriously" – medium Dutch ISP
  - "There are many invalids, but very little traffic is impacted" – very large cloud provider



### **Origin Validation vs Path Validation**

- ROA-based validation covers only part of the problem
- hardware
- Work in progress:
  - Autonomous System Provider Authorization (ASPA)
- Don't wait, start now

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022



BGPsec implements Path Validation, but too difficult for current

### Recommendations

### Create Your ROAs

- signing and validation"
- Pay attention to the maxLength
- Download a Validator, or two
- Check validation status manually: which routes are invalid?

Oleg Muravskiy RIPE NCC Days Tashkent 23 September 2022



# "My network becomes safer if you implement both

### Set up monitoring, for example BGPalerter or pmacct

### Making the Difference

- Is routing security on your agenda?
- Are you leading by example?

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022 |



# Initiate the conversation with providers and colleagues



## Recent developments

### Address Space Covered by ROAs



Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022 |







*source: <u>https://certification-stats.ripe.net/</u>* 

### Status of Routing Announcements



Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022



source: <u>https://rpki-monitor.antd.nist.gov</u>

### IPv4 ROA Coverage (all RIRs)



### Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022





AF	66%
IR	98%
KG	82%
KZ	8%
PK	98%
TJ	4%
ТМ	1%
UZ	26%

source: <u>https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html</u>

## Recent developments at the RIPE NCC



### **RIPE NCC RPKI Numbers**

- 18,414 RPKI certificates
  - More than 75% of members
- 32,839 ROAs

Oleg Muravskiy | RIPE NCC Days Tashkent | 23 September 2022 |



### More than 50% of the RIPE NCC's address space • 17% of members with certificates do not have ROAs

### **RIPE NCC RPKI Trust Anchor and Certification Authority**

### Improving security

- Finished migration to a new offline Hardware Security Module (HSM)
- Planning migration to a new online HSM later this year
- Regular penetration tests for our software
- Red-team test (overall security exercise) this year



### **RIPE NCC RPKI Trust Anchor and Certification Authority**

### Improving transparency

- Updated RIPE NCC Certification Practice Statement
  - Next version will be reviewed by the community
- All security test reports from external parties available online
- We are transparent about our priorities and publish our <u>quarterly plans</u>
- We open-sourced our <u>RPKI CA code</u> this year
  - Other parts are already open source



### **RIPE NCC RPKI Trust Anchor and Certification Authority**

### Improving auditability

- The RIPE NCC established an RPKI audit framework
- ISAE 3000 Type 1 & 2
  - Type 1: Audit the framework
  - Type 2: Audit RPKI
- We expect to have Type 1 done this year



## Questions

ncc@ripe.net





### Autonomous Systems



Oleg Muravskiy | |







### Origin AS



Oleg Muravskiy | |









### Origin AS and AS PATH



Oleg Muravskiy | |





### Origin AS and AS PATH



Oleg Muravskiy |





### Origin hijack





Oleg Muravskiy | |











Oleg Muravskiy | |



