Intro to RPKI

Contact: training@apnic.net



eSEC04_v1.0



Overview

- What is RPKI?
- Background of RPKI
- Right to Resources
- X.509 Certificates
- Route Origin Authorizations (ROA)
- What is Resource Certification?
- Creating ROA records

APNIC



SIDR Working Group

- Secure Inter-Domain Routing (SIDR)
- Its purpose is to "reduce vulnerabilities to the inter-domain routing system"
- Addresses two vulnerabilities:
 - Is an Autonomous System authorized to originate an IP prefix?
 - Is the AS-Path represented in the route the same as the path through which the NLRI traveled?
- RPKI is in the process of standardization through the Secure Inter-Domain Routing (SIDR) working group

http://datatracker.ietf.org/wg/sidr/charter/

What is **RPKI**?

- Resource Public Key Infrastructure (RPKI)
- A robust security framework for verifying the association between resource holder and their Internet resources
- Created to address the issues in RFC 4593
- Uses X.509 v3 certificates
 With RFC3779 extensions
- Helps to secure Internet routing by validating routes
 - Proof that prefix announcements are coming from the legitimate holder of the resource
- A system to manage the creation and storage of digital certificates and the associated Route Origin Authorization documents





RFCs on RPKI

- RFC 6810 The Resource Public Key Infrastructure (RPKI) to Router Protocol (January 2013) - Standard
- RFC 6480 An Infrastructure to Support Secure Internet Routing (Feb 2012) - *informational*
- RFC 6481 A Profile for Resource Certificate Repository Structure (Feb 2012) - *standard*
- RFC 6491 RPKI Objects Issued by IANA
- RFC 6493 The RPKI Ghostbusters Record
- RFC 6487 A Profile for X.509 PKIX Resource Certificate





Resource Certification Benefits

- Routing information corresponds to properly delegated address resources
- Resource Certification gives resource holders proof that they hold certain resources
- Resource holders can attest to those resources when distributing them





Benefits (Cont.)

- Resource users can 'sign' information with a digital signature, which essentially 'freezes' that information
- Any effort to alter that information results in the signature being invalidated
- Only resource holders with a properly delegated 'right of use' can generate a signature
- Routing advertisements are made with the explicit agreement of the current 'right of use' holder of the addresses being advertised.
- Prevents "Route Hijacking"
 - when an entity participating in Internet routing announces a prefix without authorization
 - Reason: malicious attack or operational mistake





"Right" to Resources

- ISP gets their resources from the RIR
- ISP notifies its upstream of the prefixes to be announce
- Upstream _must_ check the Whois database if resource has been delegated to customer ISP.





X.509 Certificate

- Resource certificates are based on the X.509 certificate format - RFC 5280
- Extended by RFC 3779 this extension binds a list of resources (IP, ASN) to the subject of the certificate





X.509 Certificate with 3779 Extension



 SIA – Subject Information Access; contains a URI that references the directory





Two Components

- Certificate Authority (CA)
 - Internet Registries (RIR, NIR, Large LIR)
 - Issue certificates for customers
 - Allow customers to use the CA's GUI to issue ROAs for their prefixes
- Relying Party (RP)
 - Software which gathers data from CAs





Route Origin Attestations (ROA)

- Certificate holder uses its private key to sign an ROA
- Verifies that an AS has been given permission by an address block holder to advertise routes to one or more fpxies without a blog.





RPKI in the RIRs

• APNIC implemented RPKI Resource Certification





APNIC Resource Certification

- A robust security framework for verifying the association between resource holders and their Internet resources.
- Initiative from APNIC aimed at
 - improving the security of inter-domain routing, and
 - augmenting the information published in the Whois database
- Verifies a holder's current "right-of-use" over an Internet resource





How it Works

RPKI Component elements and interactions







Resource Certification (APNIC)

- Verify signed data using the signer's public key
- Verify public key through a chain of interlocking certificates that connect a Trust Anchor to the signer's public key certificate.
 - This is what we refer to as RPKI
- Why it's important:
 - Routing advertisements is now verifiable





Creating ROA Records

Login to MyAPNIC, then Resources -> Certification

MyA	PNIC (::)::::::::::::::::::::::::::::::::::	APNIC ntacts My Profile Log out
	Home Resources Administration Training Tools IPv4 IPv0 Asiv Whois updates Certification Maintainers IRTs 0	Correspondence
	Home / Resource management	
Reminder	Resource management	Useful links
Please register your whois maintainer.	Internet resources	Resource management
	View and manage resources	Assignment window
	Whois database updates	FAQ
	Add/Update/Delete Whois objects	
	Resource request forms	
	IPv4 addressesIPv6 addressesAS numbers	
	Resource transfer/return	
	 Transfer resources into another account Receive resources into my account Transfer pre-approval Return resources to APNIC 	
	Resource certification	
	Manage certification	





Adding ROA Records

• Simple view and add using the form

MyAF	PN	IC	(yr:	:::ʃ:::ʃ::) Sheryl [APNICT	RAINING-4	APNIC
	Home	Voting	Resources	Administration	Training	Tools
	IPv4	IPv6 AS	N Whois upd	dates Certification	Maintaine	ers IRTs Correspondence
Home / Resources / RPKI						
RPKI						

ROA Configuration

Origin ASN		Prefix		Max Length			Add	Add & clone Clear
All Changes		Items per page 1	0	Search by AS or IP				Certified Resources
Origin AS	^	Prefix	^	Max Length				61.45.248.0/23
12345		61.45.251.0/24		24	Ĩ	.		61.45.251.0/24
17821		61.45.248.0/23		24	í	1		61.45.253.0/24
				Showing 1 to	0 2	of 2 entrie	s	203.176.189.0/24
Commit				-	<	1 of 1	>	2001:DF0:A::/48
								2406:6400::/32





Deleting ROA Records

MyAl	PN			Sheryl [APNICI	RAINING-A	U] Manage	APNI Contacts My Profi	C le Log out	Constants
	Home	Voting	Resources	Administration	Training	Tools			
	IPv4	IPv6 ASN	Whois up	dates Certification	Maintaine	rs IRTs	Correspondence		
Home / Resources / RPKI									
RPKI									
ROA successfully marked	for removal	(12345, 61.45	.251.0/24, 24).	Remember to commit	your changes.				×

ROA Configuration

Origin ASN	Prefix	Max Length	Add	Add & clone Clear
All Changes	Items per page 10	\$ Search by AS or IP		Certified Resources
Origin AS	Prefix A	Max Length	A V	61.45.248.0/23
12345	61.45.251.0/2 4	24	С	61.45.251.0/24
17821	61.45.248.0/23	24	<u>ش</u>	61.45.253.0/24
		Showing 1 to	2 of 2 entries	203.176.189.0/24
Commit			< 1 of 1 >	2001:DF0:A::/48
				2406:6400::/32





APNIC Helpdesk Chat



(∷**(∷(∷**)



Thank You!

End of Session



