Generating a Letter of Agency to Reflect RPKI Validity

draft-martin-grow-rpki-generated-loa-00

Joe Abley, Algin Martin – Cloudflare – 4 November 2024 – IETF 121 (remote) – grow

Problem Statement

- Customers bring their own IP addresses to network and service providers and want to associate them with the services they are buying
  - Customers expect the service providers to originate prefixes on the customer's behalf
  - Service providers need authorisation to make sure they are not complicit in some kind of terrible prefix hijacking expedition
- The authorisation would ideally be meaningful and verifiably-secure
- The process of obtaining and checking authorisation would ideally be low-friction, robust and safe to automate

What Happens Today

- Service providers have a variety of heuristics they can use to construct a sense of whether a request to originate a prefix is authorised
  - RIR assignment/allocation data (e.g. via RIR whois server)
  - IRR routing policy data (e.g. published route/route6 objects)
  - Current and historical routing data (e.g. what routes are and have been originated before)
  - Unauthenticated documents that contain opinions (e.g. LOAs, LOIs)
  - RPKI-signed objects (ROAs, ASPAs, signed checklists)

What Happens Next, Today

- Service Provider onboards the prefix
  - Publishes information in the IRR about it, as appropriate
  - Sends LOA to adjacent networks as a record of authorisation
- Service Provider can now originate the prefix with some hope that it will propagate
- Service Provider should keep checking things during the period during which the prefix is onboard and available to be originated
  - e.g. continue to verify published data from RIR/IRRs, do RPKI validation

This is Not Great

- Of all of those heuristics, only RPKI validity checks are robust
  - LOAs might as well be smartphone photos of vague statements written in crayon on dirty napkins
  - Processing of all of these things are manual for both the service provider and the customer
  - Humans make mistakes, and manual processing is not a robust defence against route hijacking
- An automated, secure process is better than a manual, insecure process

RPKI to the Rescue

- In many common scenarios, one or more RPKI-signed objects provide clear, cryptographically-validatable authorisation for a service provider to originate a prefix on behalf of a customer
  - ROAs, or ROAs + ASPAs
  - Signed Checklists can be used as proof of binding between a prefix and a customer identity
- But unless we have a flag day, a service provider still needs a way to communicate the authorisation inferred through RPKI to adjacent operators

This Document

draft-martin-grow-rpki-generated-loa-00

- If we as service providers confirm authorisation to originate a prefix for a customer using only RPKI-signed objects, then
  - We don't have to care about LOAs (hooray!)
  - We don't have to collect a LOA from customers (more hooray!)
  - We still have adjacent network operators who expect to receive a LOA from us
- This document aims to record consensus about what it is reasonable for us to send to peers and transit providers

Motivation and a Closing Question

draft-martin-grow-rpki-generated-loa-00

- This is a problem we are looking at at Cloudflare
  - We want to implement something
- We think it would be helpful to have consensus about what we should send in place of an LOA when the customer didn't provide one
  - We think there are kind-of interop reasons for this
  - We also thinks that writing this stuff down would help us all move towards a more secure and automatable, RPKI-consuming world
- Is grow interested in working on this?