Considerations on RPKI Overclaiming

John Curran

Geoff Huston

CA Operations

- A CA may encounter a situation where it is necessary to re-issue a subordinate certificate where the resources in the newly issued certificate are smaller than the previous certificate, and subsequently revoke the previously issued certificate
- In this scenario, if the actions of the CA are not adequately coordinated with subordinate CAs then there is a risk of the subordinate CA operating with an “overclaiming” certificate

“Overclaiming” Certificates

- RFC3779 and RFC6487 define a validation process that causes relying parties to consider an “overclaiming” certificate to be not valid
- This would cause the certificate, and any attestation that relies on this certificate not to be considered by the relying party when forming their model of which resources are “valid”
- In a partial deployment model, this is mostly harmless, as the resources would be considered to be “unknown” rather than “invalid”
- The one exception to this is the situation of more specific routes of an aggregate with a valid ROA
  - When the certificate of the ROA of a more specific of an valid aggregate (i.e. the aggregate is authorized by a valid ROA) is not able to be validated then the route is to be considered “invalid” (RFC6483)

How common are “overclaiming” certificates?

- Reports from IETF 90 indicate that this is an uncommon situation so far
- The “Validation Reconsidered” draft <draft-ietf-sidr-rpki-validation-reconsidered> postulates that there are intermediate states in a resource transfer that may give rise to such “overclaiming” of certificates, but the analysis in this draft is not detailed and the motivation for changing the validation algorithm is not based in operational experience with overclaiming of certificates

Risks

- “Overclaiming” for CAs that are close to the Trust Anchor for the RPKI could create a consequence of unvalidatable ROAs for the period of extant overclaimined certificates
- In an environment of partial deployment of RPKI in routing the consequences of this situation may result in de-pref of routes (“valid” to “unknown”) and there may be some instances of route discard (more specifics routes: “valid” to “invalid”)
- Such risks could impact the level of confidence in adoption of routing security and/or preclude the eventual ability to move to requiring “valid” routes

Next Steps?

- Evaluate the current CA operational procedures for managing transfers and RPKI certificates and document risks and mitigations?
- Develop a standard procedure for certificate management during resource transfer?
- Review the need to alter the RPKI validation process along the lines of the “validation reconsidered” draft?