RPKI and Routing Security

ICANN 44

June 2012

Today's Routing Environment is Insecure

- Routing is built on mutual trust models
- Routing auditing requires assembling a large volume of authoritative data about addresses and routing policies
  - And this data does not readily exist
- We have grown used to a routing system that has some "vagueness" at the edges

Telling “Good” from “Bad”

Can we set up a mechanism to allow an automated system to validate that the use of an address in routing has been duly authorized by the holder of that address?

This looks a lot like an application of public/private key cryptography, with “authority to use” conveyed by a digital signature

- Using a private key to sign the authority, and the public key to validate the authority
- We could use a conventional certificate infrastructure to support public key validation at the scale of the Internet
- But how can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

- Use the existing address allocation hierarchy
  - IANA, RIRs, NIRs & LIRs, End holders
- Describe this address allocation structure using digital certificates
- The certificates do not introduce additional data – they are a representation of registry information in a particular digital format

Resource Certificates

- A resource certificate is a digital document that binds together an IP address block with the IP address holder's public key, signed by the certification authority's private key
- The certificate set can be used to validate that the holder of a particular private key is held by the current legitimate holder of a particular number resource – or not!

- Community driven approach
  - Collaboration between the RIRs since 2006
  - Based on open IETF standards
    - Based on work undertaken in the Public Key Infrastructure (PKIX) and Secure Inter-Domain Routing (SIDR) Working Groups of the IETF

The RPKI Certificate Service

- Enhancement to the RIR Registry
  - Offers validatable proof of number holdership
- Resource Certification is an opt-in service
  - Number Holders choose to request a certificate
    - Derived from registration data

A Number Resource PKI

- The RPKI is a service that offers a means to validate attestations about addresses and their current holder
  - The ability to validate assertions about an entity being the holder of a particular address or autonomous system number
    - "I am the holder of 1.1.1.0/24"
  - The ability to make more reliable routing decisions based on signed credentials associated with route objects
    - "I authorise AS 23456 to originate a route to 1.1.1.0/24"

Community Concerns

1. External Intervention
   - Certificate Issuer could be forced to tamper with the certificate contents (court order)
     - This is no different from the existing external intervention factors with the registry contents itself – the certificates do not add or detract from the issues here
2. Security
   - The certificate system could get compromised (hack, error, etc.)
     - Much effort has been invested in industry best practices of key management and certificate issuance system integrity by the RIRs
3. Resilience
   - The system could suffer from a failure
     - Signed data allows for widespread replication of the data itself. The signature can be used to validate the currency and legitimacy of the data.

Current Activities

- Certificate Infrastructure
  - Integration of Certificate Issuance Systems into production services
  - Signing and validation service modules as plugin modules for other apps
  - Tools for the distribution and synchronization of the certificate store
- Secure Routing Systems
  - Specification of AS Path signing extensions to BGP

Questions?