RPKI with rpki.net TooIS

Muhammad Moinur Rahman

RPKI: Introduction

- Tutorial
- Target audience
  - Knowledge of Internet Routing(specially BGP)
  - Familiar with any IRR Database
  - No need to know Cryptography
  - Basic knowledge of PKI(Public Key Infrastructure)
- Layout
  - Theory
  - Handson Lab using rpki.net tools on Cisco IOS, Cisco IOS-XR and Juniper

Historical Incident

- November, 2012 – Google traffic affected in AP region due to hardware failure of Moratel
- Pakistan Telecom and Youtube incident
- 7007 accident, UU/Sprint for 2 days

Historical Incident (Thinks to Consider)

- For theory of positivity let’s call all these as Mis-Origination
- Traffic Hijacking or Prefix Hijacking assumes Negative intent

Historical Context

- 1986 – Bellovin & Perlman identify the vulnerability in DNS and Routing
- 1999 - National Academies study called it out
- 2000 – S-BGP – X.509 PKI to support Secure BGP - Kent, Lynn, et al.
- 2003 – NANOG S-BGP Workshop
- 2006 – RPKI.NET(for ARIN) & APNIC start work on RPKI. RIPE starts in 2008.
- 2009 – RPKI.NET Open Testbed and running code in test routers

Current Trend

- Filtering limited to the edges facing the customer
- Filters on peering and transit sessions are often too complex or take too many resources
  - Do you filter?
- A lot depends on trusting each other
  - Daily examples show this is no longer enough

When filtering is not enough ..

- A lot of different registries exist(Nearly 40), operated by a number of different parties:
  - Not all of them mirror the other registries
  - How trustworthy is the information they provide?
- The IRR system is far from complete (RPSL lives with RPSLNG) but no further development.
- Resulting filters are hard to maintain and can take a lot of router memory

Goals of RPKI

- Running a Secured Internet for the end users
- Reducing routing leaks
- Attaching digital certificates to network resources
  - AS Numbers
  - IP Addresses
- Allowing ISPs to associate the two
  - Route Origin Authorizations (ROAs)
  - Can follow the address allocation chain to the top

RPKI Accomplishes

- Allows routers or other processes to validate route origins
- Simplifies validation authority information
  - Trust Anchor Locator
- Distributes trusted information
  - Through repositories

Public Key Concept

- **Private key**: This key must be known only by its owner.
- **Public key**: This key is known to everyone (it is public)
- **Relation between both keys**: What one key encrypts, the other one decrypts, and vice versa. That means that if you encrypt something with my public key (which you would know, because it's public :-), I would need my private key to decrypt the message.
- Same alike http with SSL aka https

PKI in IRR

- The RIRs hold a self-signed root certificate for all the resources that they have in the registry
  - They are the trust anchor for the system
- That root certificate is used to sign a certificate that lists your resources
- You can issue child certificates for those resources to your customers
  - When making assignments or sub allocations

Route Origination Authorization (ROA)

- Next to the prefix and the ASN which is allowed to announce it, the ROA contains:
  - A minimum prefix length
  - A maximum prefix length
  - An expiry date
- Multiple ROAs can exist for the same prefix
- ROAs can overlap

RPKI Protocols

- Certificate Authority
- Relying Party/Origin Validation

Result of Check

- **Valid** – A matching/covering ROA was found with a matching AS number
- **Invalid** – A matching or covering ROA was found, but AS number did not match, and there was no valid one
- **Not Found** – No matching or covering ROA was found

Policy Override Knobs

- Disable Validity Check Completely
- Disable Validity Check for a Peer
- Disable Validity Check for Prefixes
- When check is disabled, the result is “Not Found,” i.e. as if there was no ROA

How to run CA?

- Open Source Software to run a member CA
  - Use the LIR as parent CA (trust anchor)
  - Generate and publish Certificate yourself
- LIR Hosted Platform
  - All processes are secured and automated
  - One click set-up of Resource Certificate
  - WebUI to manage Certificates in LIR Portal
  - All the major LIR do have RPKI/Resource Certification configuration options in their portal

How to run RP?

- Rpki.net tools (Both CA and RP)
- RIPE/NCC (Both CA and RP)
- RTRLIB (RP Only)
- APNIC (CA Only)

Validation in Practice

- All certificates and ROAs are published in a repository and available for download
- Software running on your own machine will periodically retrieve and verify the information
  - Cryptographic tools check all the signatures
- The result is a list of all valid combinations of ASN and prefix, the “validated cache”

RPKI Support in Routers

- The RPKI-RTR Protocol is an IETF Internet Draft
- Production Cisco Support:
  - ASR1000, 7600, ASR903 and ASR901 in releases 15.2(1)S or XE 3.5
  - Cisco Early Field Trial (EFT):
  - ASR9000, CRS1, CRS3 and c12K (IOS-XR 4.3.2)
- Juniper has support since version 12.2
- Quagga has support through BGP-SRX

RPKI-Router Integration

- Local Validator Tool (RP) feeds RPKI capable router with processed data set
  - Router does not do the crypto!

RPKI Workflow

- Creates a repository
  - RFC 3779 (RPKI) Certificates
  - ROAs
  - CRLs
  - Manifest records

RTR Workflow

- Storing ROA cache using RTR protocol which can be downloaded from the validator and kept available in memory
- Validate with ROA cache data inside the router where BGP process will check each announcement and label the prefix
- Propagate RPKI validation result with iBGP for other router (Sending/Receiving BGP Extended Community must be enabled) to make a decision (Modify pref or filter) based on it

Who is deciding what to do?

- The Validator is a tool which can help you making decisions about routing
- Using it properly can enhance the security and stability of the Internet
- It is your network and you make the final decision

Repository View

```
root@rpki# ls /ba/03a5be-ddf6-4340-a1f9-
1ad3f2c39ee6/1:
ICcaIRKhGHJ-TgUZv8GRKqkidR4.roa
cKxLCU94umS-qD4DOOkAK0M2US0.cer
dSmerM6uJGLWMMQTl2esy4xyUAA.crl
dSmerM6uJGLWMMQTl2esy4xyUAA.mnf
nB0gDFtWffKk4VWgln-12pdFtE8.roa
```

- A Repository Directory containing an RFC3779 Certificate, two ROAs, a CRL, and a manifest

Using a Repository

- Pull down these files using a manifest-validating mechanism
- Validate the ROAs contained in the repository
- Communicate with the router marking routes “valid”, “invalid”, “unknown”
- Up to ISP to use local policy on how to route

RPKI Workflow

- RPKI Web interface -> Repository
- Repository aggregator -> Validator
- Validated entries -> Route Checking
- Route checking results -> local routing decisions (based on local policy)

RPKI Caveats

- When RTR session goes down, the RPKI status will be not found for all the bgp route after a while
  - Invalid => not found
  - we need several RTR sessions or care your filtering policy
- In case of the router reload, which one is faster, receiving ROAs or receiving BGP routes?
  - If receiving BGP is match faster than ROA, the router propagate the invalid route to others
  - We need to put our Cache validator within our IGP scope

Who do we trust?

Can we trust the *IR for hosting our Private Keys?

Two digital certificates have been mistakenly issued in Microsoft's name that could be used by virus writers to fool people into running harmful programs, the software giant warned Thursday.

According to Microsoft, someone posing as a Microsoft employee tricked VeriSign, which hands out so-called digital signatures, into issuing the two certificates in the software giant's name on Jan. 30 and Jan. 31.

FAQ: Microsoft's security breach and how it affects you
story

Such certificates are critical for businesses and consumers who download patches, updates and other pieces of software from the Internet, because they verify that the software is being supplied from a particular company, such as Microsoft.

RPKI: Further Reading

- RFC 5280: X.509 PKI Certificates
- RFC 3779: Extensions for IP Addresses and ASNs
- RFC 6481-6493: Resource Public Key Infrastructure

Demo: Two Parts

- Creating ROAs in LIR Portal
- Validating and Configuring routers to make a decision for a prefix

RPKI: Questions

```
Contact
    person:         Muhammad Moinur Rahman
    address:        The Alliance Building. (6th Floor),
    address:        63 Pragati Sharani, Baridhara,
    country:        BD
    phone:          +8801977881132
    e-mail:         moin@1asia-ahl.com
    nic-hdl:        MMR13-AP
    notify:         moin@1asia-ahl.com
    mnt-by:         MAINT-BD-1ASIAAHL
    changed:        moin@1asia-ahl.com 20121128
    source:         APNIC
```