Towards a Framework for Evaluating BGP Security

Olaf Maennel, Iain Phillips, Debbie Perouli, Randy Bush, Rob Austein, Askar Jaboldinov

CSET

August 6, 2012
Resource Public Key Infrastructure (RPKI)

Security was not a concern in the first days of the Internet. Things have changed...

2006 - 2008: RPKI Design, done mostly outside the IETF
2008 - present: RPKI in IETF sidr working group

Detect and prevent \textit{mis-origination}:
a prefix is originated by an AS which does not own it.

BGP announcement for 147.28.0.0/16
AS Path: 16509 1239 2497 234

hijacked or misconfigured
Large Scale Testing

- Implementations of the RPKI exist. Some initial tests have been performed.

- The code is deployed by some RIRs and ISPs.

- Not enough evidence that deployment will scale to the Internet of 2020.

- Propagation times of the RPKI objects (like certificates) critical for the success of the system; could vary based on scale.

  How do times change with more tiers of ASes, more layers of caches per AS, more load per certification/publication point or cache, ...?

- TestBed experiments needed to answer the question: does the proposed framework for AS origin validation scale?
## RPKI High Level View

### Certification
- Who is the legitimate owner of a prefix?
- Who is authorized to announce it in BGP?

### Publication
- Who publishes, and how, the Route Origin Authorizations (ROAs)?

### Verification
- How do the relying parties know which announcements to trust?
Our Challenges

1. How do we deploy a testbed of hundreds of machines with RPKI configurations?

2. Interested in testing real vendor code (routers) and infrastructure software (rpki).

3. There are many separate but coordinated device configurations that need to be created; a time consuming, repetitive and error prone task.
StarBED: ~1000 Physical Machines
Experiment Setup

- Machine resources:
  - StarBED VMs hosting caches and Certification Authorities (CAs)
  - Junosphere for routers (currently ~50 virtual routers)

- Configuration:
  
  Extend AutoNetkit to generate automatic configurations not only for routers but also RPKI servers and caches

  Design the abstractions needed for RPKI.
Reduce the Load to the Publication Points

Extremely Large ISP Deployment
What does a Tier 1 AS look like?
What is Propagation?

- The time from when a CA publishes an object (Cert or ROA) to when a Relying Party receives it.

- A Relying Party is a validated cache or a router via the rpki-rtr protocol.

- Measured by caches and routers logging every received object.
What do Current Topologies look like?

672 caches (81 gatherers)

736 virtual machines total
Early Results

pubd-to-caches

Cumulative density vs. time (min)
Conclusion

- BGP security is a concern. The RPKI is a solution.

- We have designed the abstractions needed for RPKI to be tested in large experiments.

- We have automated the configuration of the machines running RPKI code.

- We are performing large scale experiments.