Effect of RPKI Deployment Scenarios
(work in progress)

Alexandru Ștefănescu, Benno Overeinder
Guillaume Pierre

alex@NLnetLabs.nl

NLnetLabs
Vrije Universiteit Amsterdam
Outline

• Our objectives
• Approach – emulation on a cluster
• Protocol abstraction level
• The simulator
• Expected results
Goals

- Study effect of BGP security deployment scenarios
- Find out order in which to start securing ASs for maximum benefit
- Better protocol understanding: relation between no. of secured ASs and secured routes
  - Impact of securing just biggest ASs (e.g. Tier 1)
  - How important is securing CDNs?
Approach

- Allow for easy implementation of security solutions
  - We can emulate practically any proposed security additions
  - Focusing on route origin validation in BGP
- Do not perform crypto computations, but emulate
- Abstract what you can, but run everything in (scaled) real-time
- Gather as much real-world data/scenarios and run the simulation upon them
Model

• Abstract protocol and network (existing simulator):
  – no physical network modeling, 1 AS = 1 node (ignore IBGP)
  – standard BGP features: explicit prefix tables, announce and withdraw messages, route propagation according to policies, etc.

• Security model:
  – tag BGP messages as being “validated” or not
  – security policies assigned to ASs individually
    • most interesting: *favor secure routes on tie*
Our software

• Enhanced version of simulator by M. Wojciechowski
• Java simulator running on homogeneous cluster
• Each AS is a separate thread
• Uses network annotated adjacencies from CAIDA
• Allows easy tweaking of BGP behavior and security policies
Variables

- Running scenarios:
  1. Assign security policies
  2. Propagate prefixes
  3. Count validated route announcements

- Factors:
  - What if topology changes?
  - What is the impact of different types of security policies?
  - What is the impact of different security policy distributions?
  - How does it differ when prefix announced by stubs vs. large ASs?
Envisioned Results

- Continue previous work
  - Sharon Goldberg et al.
  - Jennifer Rexford et al.

- More detailed simulations of security deployment

- Guide for favorable turnover for investments in BGP security

- Results show trends instead of specific AS behavior due to many levels of abstractions
Directions

- Perform as many tests as possible using various deployment scenarios
  - Open to suggestions, contact us!
- Include time dynamic experiments in study
  - Convergence time of validated vs. unknown prefix announcements
- For more information:
  - {alex, benno}@nlnetlabs.nl
  - http://www.nlnetlabs.nl/projects/bgpsim/
References


3. CAIDA - Cooperative Association for Internet Data Analysis - http://www.caida.org/home/

4. The Distributed ASCI Supercomputer 4 - http://www.cs.vu.nl/das4


Questions?