ISP Route Filtering: Responsibilities & Technical Challenges

Richard Steenbergen - nLayer Communications
Ruediger Volk - Deutsche Telecom
Warren Kumari - Google
Larry Blunk - Merit Network
Danny McPherson - Arbor Networks
Panel Objectives

• Discussion:
  – what’s changed related to inter-domain route filtering over the past 15 years
  – how we can improve inter-domain prefix filtering
  – what operators should be doing, what responsibilities do you have today

• Focus is on validating prefix announcements, NOT transport connection protection
15+ Years, What’s Changed?

• More stale IRR data
• Less (%) employment of inter-provider filtering
• Still no verifiable source for who owns what, who’s authorized to originated what
• An order of magnitude more meat computers with BGP router enable access
• Much greater reliance on Internet availability

• Summary: Security of routing system has deteriorated, not improved
The IRRs

- IRRs decentralized - ~55 IRRs currently
  - Operated by RIRs, operators, other, none authoritative
- Perception: data is largely unusable, insecure, stale - Do people ever actually delete IRR objects?
- Customer issues - don’t understand or want to use IRRs, ISPs proxy
- Insecure IRR update models (++RIPE)
- Tools to configure based on IRR data, internal database - ISPs should have these functions fully automated
- Inter-IRR communications, which are trustworthy, how is this enumerated in deployed policy
- Timing issues, race conditions
- Full route policy enumeration
- Special case policies (e.g., more-specifics with blackhole communities)
- Use of IRRs cost money$$
IRR & Routing System

- What’s delta from RIR - > IRR -> routing system?
- NEMECIS:
  - “RIPE has best IRR data set”
  - “Data in IRR is useful”
- No ‘RIR x Origin AS’ association data today

Data Above From NEMECIS:
- www.cs.ucr.edu/~michalis
- www.cs.ucr.edu/~siganos
IP Address Allocation, Assignment, and IRR Conceptual Model

Objects generated from Route Origination Authorization (ROA) data from RPKI by RIRs most trustworthy

RPKI introduces infrastructure for formally verifying who owns what
Constructing Validated IRR Objects from RPKI

• IRR data generated from RPKI provides trustworthy source, RIRs operate IRRs
• What other IRR objects need more security wrapped around them (e.g., as-set and aut-num)
• Secure IRR update mechanisms
• Do other components in the model need secured?
Routing Protocol Issues

• Timing issues associated with route announcements and new policy application, newer techniques ease old constraints
  – Soft reconfiguration
  – Adj-RIB-In storage & implementation
  – BGP Route Refresh

• Eases much of this burden - no need to bounce route at source, or reset BGP sessions
Router Issues

• Ability to handle per-peer explicit prefix lists (500k or more) - where do things break?

• Policy specification language, e.g.,:
  – Transit explicit /24 prefix
  – Accept /24-32 with community $n$
  – How to express?

• What’s processing hit, process prioritization during configuration loads?

• Can policy also be used for datapath (e.g., BCP 38) or must another be defined?

• New policy application (e.g., immediate application versus periodic, etc..) - e.g., Cisco versus Juniper configuration model?

• Where’s bottleneck?

• RICHARD: SLIDE FROM SCHOLL?
Other Related Functions

- General filtering stuff today
- Max prefix - what about full possibilities enumeration?
- Prefix length-based filtering (/24 longest generally)
- AS_PATH based
- Customer communities based stuff (e.g., blackholing) - separate session?
- Prevent /8 hijacking? announce two /9s!
Panel/Community Questions
Achieving Incremental Deployment

• With:
  – A tool like NEMECIS that diffs RPKI IRR and internal/third-party IRR data v. routing system state
  – RPKI as formally verifiable source to construct IRR data
  – Tools to manage internal database for router configuration
  – cont…
Achieving Incremental Deployment (cont.)

• What else is gating deployment:
  – Bi-lateral deployment inter-domain prefix-based filtering policies - incremental benefit
  – At least ORDERED preference model where RPKI IRR routes preferred over non-RPKI, then subsequent diminishing preference based on source
  – Would really like to account for no acceptance of more-specifics for RPKI routes, but this might become problematic until full IRR model is employed
Incentive Models

- Tragedy of the commons?
- There’s incremental benefit with each new peer that you filter - Agree or disagree?
- Do you consider this in peering agreements today, or only customer side?

- Every ISP MUST filter customer BGP route announcements, no excuses! Agree or disagree?
IRR Questions

• Is IRR at end of life and only incremental changes and move to direct RPKI model?
• Or build RPKI-seeded IRRs from RIRs and tools to expand their use
• “Is IRR system too complex for most users?
  – Expression language enables extremely complex configurations, perhaps at expense of being able to easily generate prefix lists
  – Software to parse it can barely be compiled, let alone run
  – Thereby slowing adoption rate among ISPs”
• Give up….
Miscellaneous Considerations

• Availability and security of RPKI infrastructure and IRRs
• Who are RPKI Trust Anchors and what impact does that have on technical, political considerations?
• Are we trading autonomy for security with RPKI model?
• Where are ALL the RIRs with implementation of RPKI data to construct validated IRR objects?
Other?