Network Security Service Development at DE-CIX: Blackholing and RPKI-Light / BGPSec-Light

T. King, R&D DE-CIX
Agenda

- Blackholing
- RPKI-Light
- BGPSec-Light
Blackholing
Motivation: The Problem: Massive DDoS
Motivation: A Solution: Blackholing

DDoS

BGP:
More Specific Blackhole Announcement

IXP
Number of ASNs (≈ Customers)
Number of Prefixes Blackholed

![Graph showing the number of new announcements over time.](#)
Todos

• Implementation of Blackholing feature
• Simple trigger to activate blackholing: commonly agreed Blackholing BGP community
• Dedicated Blackholing Route-Server
Motivation: Different Triggers for Blackholing

- Different triggers for Blackholing at IXPs (selection):
  - DE-CIX Apollon: Blackhole IP Address: FRA: 80.81.193.66, NY: 206.130.10.66
  - Netix: Blackhole Community: 65499:999
  - MSK-IX.ru: Blackhole Community: 0:666
  - NIX.CZ: Fenix: RTBH
  - TPIX.pl: Blackhole Community: 29535:666

Policy control at route servers

- Different triggers for Blackholing at ISPs (selection):
  - Init7: Blackhole Community: 65000:666
  - Team Cymru: Blackhole Community: 64496:666
  - Hurrican Electric: Blackhole Community: 6939:666
  - NTT: Blackhole Community: 2914:666

- Proposal: One commonly agreed way to trigger Blackholing at IXPs and ISPs -> Internet Draft

#9
Evolution

2014:
• Discussion about commonly agreed Blackhole community in KG IIS meetings
• Euro-IX tech mailing list: Discussion on commonly agreed Blackhole community
• A solution was selected: Blackhole BGP Community: 65535:666
• 25th Euro-IX Forum: Presentation and panel about Blackholing
• Work on an “Internet Draft” started. Authors: King, Dietzel (DE-CIX), Döring (SpaceNet), Hankins (Alu), Jiran (NIX.CZ), Kritski (NetIX), Seitz (STRATO)

2015:
• Draft of “Internet Draft” discussed on the Euro-IX tech mailing list
• “Internet Draft” Version 00 submitted to IETF GROW working group
• Discussion on the GROW mailing list and during the IETF 93
• Requests from Euro-IX and GROW:
  — Also add ISPs
  — Be more specific about “Operations Recommendations”
• Version 01 of the “Internet Draft” released (above requests applied)
• Call for “Working Group” adaption (result is pending – looks good?)
Next Steps

• We need more feedback -> Release new versions: Repeat

• Last Call right before IETF 94 -> RFC?
Dedicated Blackholing Route-Server

• Discussion in KG IIS
• Discussion on the tech mailing list
• Implementation is ongoing
• RFS: Q1/2016
RPKI-Light
RRKI-Light

• RPKI: Origin validation (Is AS x authorized to originate a route for IP prefix y?)
• Discussion in KG IIS
• AMS-IX and DE-CIX are already working on it
• Open issues:
  – Acceptance
  – Implementation: Standardized signaling
RPKI Deployment

608,704 Unique IPv4 Prefix/Origin Pairs

- not-found (573,421)
- valid (31,901)
- invalid (3,382)

invalid 0.56%
valid 5.24%
not-found 94.20%
RPKI Deployment: DE-CIX NYC

• Total Prefixes: 48328
• Prefixes Valid: 33 (0.06%)
• Prefixes Invalid: 2593 (5.304%)
  – Prefixes Invalid AS: 2591 (5.3%)
  – Prefixes Invalid Length: 2 (0.004%)
• Prefixes Not Found: 45702 (94.5%)
RRKI-Light

AS1: 192.168.0.0/16

Route-Server

AS1: 192.168.0.0/16

BGP community: RPKI valid

Advantage: Routers not capable of RPKI validation are enabled to benefit from RPKI security.
RPKI-Light Implementation

• Idea: Standardize RPKI-Light signaling for IXPs
• Implementation details:
  – Extended community: Non-transitive flag?
  – One well-known community for RPKI (valid, invalid, unknown)?
  – Should the AS of the IXP be part of the extended community?
BGPSec-Light
BGPSec-Light

• BGPSec: a mechanism for providing path security for BGP route advertisements
• BGPSec does not support route-servers at IXPs (https://tools.ietf.org/html/draft-sriram-bgpsec-design-choices-08#section-7.4)
• Are you aware of this?
• How do you handle this?
• Should we try to find a solution for this?
Thank you!

Please provide feedback: