RPKI Deployment: Status, Challenges and the Learning-Validator

Amir Herzberg
Bar Ilan Univ, Fraunhofer SIT, Univ of Connecticut

Joint project with
Yossi Gilad, Tomas Hlavacek, Yafim Kazak, Refi Peretz, Michael Schapira and Haya Shulman,
RPKI Deployment: Agenda

• RPKI in a foil
• ROA adoption: trends
• Wrong ROA: causes and damages
• ROV adoption status, challenges
• Impact of partial ROV adoption
• Improving deployment
  • ROAlert.org
  • The Learning Validator
  • Demo
• Conclusions
RPKI: Resource Public Key Infrastructure

- IETF standard [RFC 6480];
  main goal: prevent (sub)prefix hijacks (false origin domain)
- Idea: issue (signed) Route Origin Authorization (ROA):

```
Prefix: 1.2.0.0/16
Origin: 333
Max-length: 20
```

- For simplicity, we ignore signing details
- Domains should do Route Origin Validation (ROV):
  - Drop BGP announcements where origin conflicts with ROA
  - I.e.: Origin is not 333 or more specific than /20
ROA Adoption History

Drop BGP announcements ➔ lose (good?) traffic...
So, how many domains do Route Origin Validation?

Announced without ROA: 647,192 (93%)
Valid ROAs: 43,796 (6.3%)
Wrong ROAs: 5,015 (0.7%)

About 10% wrong ROAs!! Consistently!!
Wrong ROAs??

- Requires **both** authorizations (ROAs) and validation (ROV)
- Risk: ROV with **Wrong ROA** → drop legit-yet-invalid announcements
  - Does wrong-ROAs happen? – Typical, real-life example:

Legend:
- Resource Certificate
- Wrong ROA
- Legit-yet-Invalid BGP Announcement

- **194.2.0.0/15** Domain 3215
- **194.2.35.0/24** Domain 1272 (Danone)
- **194.2.155.0/24** Domain 8361 (Ubisoft)
- **194.3.118.0/24** Domain 34444 (Eutelsat)
Measuring Adoption of Route Origin Validation

- Challenge: no direct way to measure the adoption of ROV ➔ no published measurements
- Idea: use Route-View-project’s BGP-collectors – and wrong ROAs!
- Observation: if collector receives invalid announcement ➔ Entire route does not enforce ROV!
Measuring Adoption of Route Origin Validation

- Challenge: no direct way to measure the adoption of ROV ➔ no published measurements
- Observation: if collector receives invalid announcement ➔ Entire route does not enforce ROV!

At least 80 of 100 largest domains do not enforce ROV!
Can we measure more precisely?
Better ROV Measurements...

• Dependency on existing wrong ROAs may be misleading
• More reliable: **publish** correct/wrong ROAs (same origin)
• Three different controlled experiments, multiple times:
  • Use RouteView Collectors (as before)
  • Use Trace-route to RIPE atlas probes
  • Use `echo` from servers (ICMP ping or TCP SYN/ACK)
• Experiments still ongoing
• Initial results: **only handful of domains** enforce ROV
  • **None** of the 100 largest domains (cf. <20)
• Similar results apparently from measurements by Randy Bush and others (didn’t yet see details)
• What’s the impact of partial-deployment of ROV?
Partial Adoption of ROV: Collateral damage

• Domains **not doing ROV** might cause ROV-enforcing domains to fall victim to prefix hijacking

• **Control-Plane vs. Data-Plane Mismatch**: domain discards invalid announcement, yet data flows to attacker

---

**Domain 2** advertises both valid and invalid routes

**Domain 2** uses invalid route for subprefix ➔ traffic to 1.1.1.0/24 still hijacked!

**Domain 3** enforces ROV: discards invalid subprefix route

**ROA**: 1.1.0.0/16 Origin 1

To: 1.1.0.0/16 route: 2-1

To: 1.1.1.0/24 route: 2-666
Security in Partial ROV Adoption: Simulation Framework

- Use Internet domain topology of CAIDA
- Pick victim & attacker
- Victim’s prefix has a ROA
- Pick domains doing ROV
- Find domains sending to victim vs. domains sending to attacker

Empirically-derived topology from CAIDA. Includes inferred peering links [Giotsas et al., SIGCOMM’13]
Security with Partial ROV Adoption

- Subprefix-hijack success rate for adoption by x largest domains
- Compare: 100% vs. 25% adoption by other domains
- Significant benefit - but only if almost all large domains adopt – and most other domains adopt too
- We are very far from this!

![Subprefix hijack success rate graph]

*Expected Deployment (top ISPs)*

1. ROV adoption prob. 1
2. ROV adoption prob. 0.25
RPKI Deployment: Agenda

- RPKI in a foil
- ROA adoption: trends
- Wrong ROA: causes and damages
- ROV adoption status, challenges
- Impact of partial ROV adoption
- Improving deployment
  - ROAlert.org
  - The Learning Validator
  - Demo
- Conclusions
Fixing ROAs and ROV deployment

- **ROAlert.org**: identifying wrong ROAs
  - Also email alerts when sysadmin-email located: 40% fixed!
  - Should be deployed `officially`
- **Improved validator** (ongoing R&D with Cisco, LinkedIn, ..)
  - **Learning mode**: no blocking; identify wrong ROAs
  - **Conservative mode**: ignore wrong ROAs, respect correct ROAs
- **ROV++**: reduce collateral-damage; gives **incentive** to deploy
- **Path-end validation**
  - Easy RPKI extension prevents origin-hijacking ➔ much improved defense! [good ROI...]
  - RPKI⇌partial-BGPsec ↔ **Path-End**
  - Details: SigComm16 paper – or ask me 😊
Beyond BGP: Routing Against DoS

• BGP is limited to single fixed route
  • Easier to congest – e.g., in Denial-of-Service (DoS)
• BGP isn’t congestion-sensitive
  • Route does not depend on congestion, delays, loss
  • Slow response to link failure
• IP provides only best-effort service
  • No quality guarantees (max delay, max loss rate)
  • Quality-of-Service (QoS) extensions: only within domain
• Secure Accountable Inter-domain Forwarding
  • On going project – talk to me…
Conclusions

• Routing security: fun & important research area
• RPKI improves BGP’s security... if deployed widely
  • ➔ ROAlert and Improved validator (ROV++)
• BGPsec deployment... unlikely ?
  • ➔ Path-End instead? Effective – and deployable!
More questions?
Thanks!

42