Preliminary Results of Survey about RPKI/DNSSEC

Matthias Wählisch

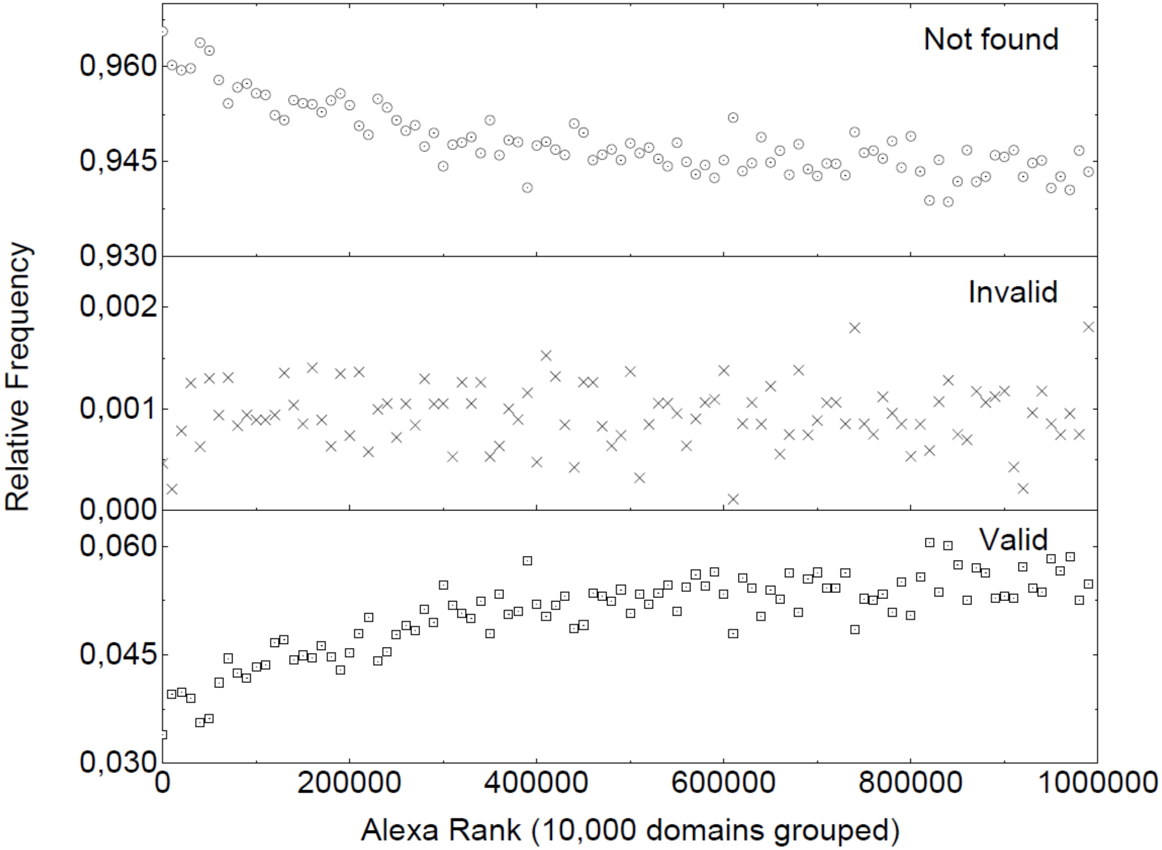
Olaf Maennel, Claudiu Perta, Thomas Schmidt, Gareth Tyson, Steve Uhlig

Motivation

- RPKI protection of web server infrastructure*
- CDNs lack RPKI deployment

Question:

Why do different types of operators adopt technologies differently?



*Preliminary results: Wählisch, Schmidt, Schmidt, Maennel, Uhlig: "When BGP Security Meets Content Deployment: Measuring and Analysing RPKI-Protection of Websites", arXiv:1408.0391, Aug. 2014

Survey Setup

- Questionnaire about RPKI/DNSSEC adoption
  - Consider both: Why operators deploy and why operators *don't* deploy technologies
  - Multiple answers were possible
- Call for participation distributed via NANOG, RIPE, IETF (Oct. 2014)

Who Participated?

- Overall 202 participants
- Per network type
  - Transit (35%), Stub (30%), CDN (13%), Tier1 (5%), other (17%)
- Per region
  - LACNIC (43%), RIPE (30%), ARIN (18%), APNIC (7%) AfriNIC (1%)

What is the main purpose of RPKI/DNSSEC?

RPKI (N=294)	**DNSSEC (N=238)**
58% Increasing security	79% Increasing security
31% Detecting misconfigs	12% Detecting misconfigs
11% Empowering authorities	9% Empowering authorities

Did you start deploying RPKI/DNSSEC?

RPKI (N=203)	**DNSSEC (N=240)**
66% No	50% No
30% Yes, create ROAs	23% Yes, sign records
4% Yes, perform validation	27% Yes, perform validation

Why did you start deployment?

RPKI (N=78)

62% Early adopters

19% Base BGP operations on validation outcome

14% Need proof-of-ownership against 3rd parties

5% Customer requests

DNSSEC (N=136)

44% Early adopters

23% Base DNS operations on DNSSEC outcome

18% Customer requests

15% Need proof-of-ownership against 3rd parties

Why did you *not* start deployment?

RPKI (N=181)

34% Waiting for experiences of others

22% No business case

18% Limited confidence in trust model

16% Not aware of RPKI

8% BGP is not our business

2% Requires to reveal business secrets

DNSSEC (N=137)

38% Waiting for experiences of others

24% No business case

15% Not aware of DNSSEC

11% DNS is not our business

10% Limited confidence in trust model

1% Requires to reveal business secrets

Some Free-text Comments

- “wrt RPKI, there is already some amount of protection with transit routing policies. […] with DNS, there are fewer protections.”
- “WE HAD A MEETING ABOUT RPKI WITH LACNIC IN BOGOTA BUT WE DON´T RECEIVE INFORMATION ABOUT DNSSEC”
- “[RPKI] Also, without a single root it's largely a joke.”

Takeaway

- To increase deployment
  - Identify early adopters
    - Security pressure is not sufficiently high
  - Report more about “What the lessons learned”
- RPKI-specific
  - 8 participants perform origin validation already, some more will coming soon
  - More concerns about the trust model compared to DNSSEC