Panel – "Security: Armed and Armored"

Adoption of DNSSEC and some notes on RPKI

Edward Lewis

APTLD 76
5 September 2019
Agenda

- DNSSEC Deployment and Choices amongst APTLD members
- DNSSEC Deployment in ccTLDs
- Some Routing Security Deployment Numbers
DNSSEC Deployment Among APTLD Members

DNSSEC Status by Member

- Signed w/DS: 29
- Signed no DS: 17
- Unsigned: 1
Some DNSSEC Cryptographic Choices Among APTLD members

Security Algorithms
- RSA-SHA1: 22
- RSA-SHA256: 17
- RSA-SHA512: 6
- ECDSA: 1
- No ZSK: 1

KSK lengths
- 2048bit: 29
- ECDSA: 17
- No KSK: 1

ZSK lengths
- 1024bit: 1
- 1280bit: 1
- 2048bit: 16
- Mixed: 9
- ECDSA: 3
- No ZSK: 1
A note on counting

- Counting APTLD members vs Counting ccTLD zones
  - These are not exactly the same
  - Why?
  - Operators may run multiple ccTLD zones
    - E.g., APTLD member operates 16 ccTLD zones, (one ASCII, the rest IDN) and they run them the same way
    - Just to pick on one example!
  - There is nothing alarming about that but it "tilts" the numbers
Adoption of DNSSEC Globally by ccTLDs

- Hard to see: there are 4 IDN ccTLDs without a DS record in right pie chart
Automatic Updates of Trust Anchors

• For the sake of "Trivia"
• The first two organizations to exercise an Automatic Update of DNSSEC Trust Anchors (RFC 5011) are APTLD members
  – ICANN wasn't the first! (Finished the first roll just last month.)
• Only three root/TLD operators have done this
IPv6 - Not all ccTLDs have IPv6 name servers
- Hard to see: 2 APTLD members do not (19 globally do not)

What is Routing Public Key Infrastructure (RPKI)/ROA?
- A means to secure Internet Routing (BGP)
- Helps identify fraudulent routing advertisements
Engage with ICANN

Thank You and Questions
Visit us at icann.org
Email: edward.lewis@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann

linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann
instagram.com/icannorg