Operational Realities of Running DNSSEC

Haya Shulman

Fachbereich Informatik
Technische Universität Darmstadt
DNSSEC Finally... Slowly Taking Off

• Many resolvers signal ``DNSSEC OK``
  • Only <5% validate

• Many (important) zones got signed
  • Forward DNS: Root, >62% TLDS, but only <1% SLDs
  • Reverse DNS (IPv4): arpa, in-addr.arpa but only <1% subdomains
Only Lack of Motivation?

• How difficult is it to deploy DNSSEC?

• Many dependencies and ... actors

• Our focus: DNS servers
Recursive Auth-Name Server (RANS)
Recursive Auth-Name Server (RANS)

Sometimes a Chain of Intermediate Proxy Resolvers...
Recursive Auth-Name Server (RANS)

>42% have more than a single intermediate resolver
Detecting RANSES

1. Send NXD query
   → Measure latency $\tau$
2. Resend same query
   → Measure latency $\lambda$
3. If $\lambda << \tau$ → RANS
   • Typically $|\lambda - \tau| > 30$ms
   • Different ASes

Detecting open recursive (ORANS)
→ Send query to our domain
→ Monitor requests on server

Shulman: Operational Realities of Running DNSSEC
Challenges of DNSSEC Adoption

• How common? Quite common...
  • >38% domains in Alexa-50K
    • >32% RANSes, >6% ORANSes
  → Significant part of DNS infrastructure

• Distribution of RANSes among Alexa-50K domains
Measure ORANSES Readiness for DNSSEC

1. Send request for a record in our signed zone → check if server receives

2. Send signed response → check if client receives

Measure non-open (RANSES) with side-channels
• see paper

25/6/2014

Shulman: Operational Realities of Running DNSSEC
RANSes Measurement Challenges

- Differentiate failure with EDNS vs DNSSEC
  - Support of DO in EDNS ≠ support of DNSSEC
- Differentiate failure with request vs response
- Identify who fails with DNSSEC
  - 1st node? 2nd node? ... Nth node? the name server?
- See paper for details
  - Also for measurements in TLDs, and in reverse DNS
- So, what is the situation?
Infrastructure Challenges

- Legacy devices = obstacle to DNSSEC adoption!!
- >69% of Alexa-50K open RANSes cannot support DNSSEC
  - > 39% fail with DNSSEC (FRMERROR/SRVFAIL)
  - > 30% strip DNSSEC
- > 18% do not support EDNS
- Higher % of RANSes
- Similar for reverse DNS
Is it Worth the Effort?

- DNSSEC prevents attacks
  - On-path (MitM) attacks (NSA, GCHQ, ...?)
  - Off-path attacks [HS12, HS13a-c, SW14]
  - Vulnerable name servers
- DNSSEC provides evidences
  - Enables forensic analysis, detection of attacks
- DNSSEC would facilitate security protocols
  - ROVER, DANE...
- **Can we do it? → Yes We Can!!**
Cipher-Suite Negotiation for DNSSEC

Amir Herzberg and Haya Shulman

Computer Science Dept. Fachbereich Informatik
Bar-Ilan University TU Darmstadt

25/6/2014 Herzberg and Shulman: Cipher-suite negotiation for DNSSEC
Servers Send Key/SIGs for ALL Supported Algs. → Large Responses!

- Intermediate devices
  - E.g., firewalls
- Transition to TCP?
  - Not all support
  - and overhead
- Low motivation to support shorter algs
  - Mandatory support of RSA
  - More algs - increase responses sizes
**Cipher-Suite Negotiation**

**Signal Ciphers in EDNS**

- Resolvers algs and priorities (new options in EDNS)
- Servers compute optimal algorithm
  - Responses signed according to that option
  - To prevent downgrade sign the supported ciphers with KSK
- Simple extension to [RFC6975]
Cipher-Suite Negotiation

• But, EDNS is transport layer (hop-by-hop)
• Intermediate caches break end-to-end cipher negotiation
  • Legacy devices cannot process new options → break cipher-suite negotiation
  • Supporting devices serve cached signatures → may not be the priority/ciphers supported by requesting clients
Cipher-Suite Negotiation

- Idea: signal in application layer
- Client concatenates ciphers as subdomains to query

```
algs.delimiter.domain: 5.13.7._cs_.foo.bar
```

- How can client know server’s algs/priorities?
  - server signals priorities in a DNSKEY record
- New alg. number for cipher options
Conclusions

• Intermediate devices impede deployment of new mechanisms
  • DNSSEC, cipher-suite negotiation, ...
• But, delegation of DNS functionality is common
  • Intermediaries are likely to persist
• More effort is required to speed adoption of DNSSEC!!
Questions?

Thank you!