DNSSEC Signing at Scale on the Edge

ólafur Guðmundsson
What we do: DNS

- Third party DNS operator for 2M+
- One of largest responders of DNS query traffic
- Largest dropper of DNS traffic in the world
- Operate large number of DNS servers at over 60 locations
- Custom DNS server developed in-house
DNSSEC launch

- Paid customers can enable it from user interface as of today
  - Soon Default on for all paid customers
- Use ECDSA P256 algorithm
  - speed and size
- Sign DNSKEY in central location
  - publish CDS/CDNSKEY as well
- All other RR’s signed at the edge
Signing speed (and size): ECDSA P256

RSA:
1181 BYTES

ECDSA:
305 BYTES
and faster
Minimal non-existent answers: “Black Lies”

• Our solution: true lies. sign a NOERROR.

• Generate a NSEC for the query name, cover minimal span, only set the NSEC and RRSIG bits ==> NXDOMAIN

missing.filippo.io. 3587 IN NSEC \003.missing.filippo.io. RRSIG NSEC
missing.filippo.io. 3587 IN RRSIG NSEC 13 3 3600 20150507190048 20150507190048 05170048 35273 filippo.io. Fb/xInfArVCMJWDBqsbBPxiKsC1ueUyBFGi5lAHbjRBGAGm8sKDJx/1YA01bKYzJep3dRgQw5hS89JukD+m8w==
Quick negative’s: the “NSEC shotgun”

- DNS Server optimized for answering exact query
- Query for TXT and there’s no TXT?
  - Set all the other bits that might exist.
- The NSEC is a valid denial for TXT, and is useless for an attacker that wants to replay it for other queries.

filippo.io. 3600 IN NSEC \003.filippo.io. A NS SOA WKS HINFO MX TXT AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG NSEC DNSKEY TLSA HIP OPENPGPKEY SPF
How expensive is online signing?

• Minimal impact
  • We have highly optimized code
  • Cutting down on number of NSEC records helps
  • Reuse signed SOA

• Key Distribution
  • You must trust your servers and have secure software distribution and boot
Our Challenge

• Required new systems
  • Central signer
  • DNSSEC health check ==> if DS is configured correctly

• Changes affected many systems we have deployed
  • DNS servers, DB, UI, secure boot,

• Supporting TLSA
  • Coming soon

• Uploading and maintaining DS records for customers
DNSSEC’s MAIN ROADBLOCK

• Registration System is out of touch with reality!!
• Need an easy way to update Parent
  • CDS/CDNSKEY publication is sufficient statement of intent!
  • Working with registrars and registers to enable DNSSEC at scale
    • will offer DNSSEC to free customers were we can update DS at parent
• CDS/CDNSKEY needs delete mode