DRAFT-PWOUTERS-POWERBIND

IETF 101, London
March 22, 2018

Paul Wouters
L. Xia (Frank)
Wes Hardaker

Two Parental Attacks

1) Serving data bypassing the child (split-DNS)

```
powerbind.nohats.ca. IN NS 1.2.3.4
powerbind.nohats.ca. IN DS 17869 8 2 f22bb[...]
powerbind.nohats.ca. IN RRSIG DS 8 3 3600 [...]

_443._tcp.powerbind.nohats.ca. IN TLSA 3 1 1 302BBD0
_443._tcp.powerbind.nohats.ca. IN RRSIG TSLA 8 3 3600 […]
```

2) Parent replacing child DS with its own

Child zone requirements

1) Public commitment by parent being a delegation-only zone
   - Publish via DNSKEY flag
2) DNSSEC transparency that does not require logging ALL DNS records with public keys
   - With above flag, we only need to log DNSKEY / DS records or their NSECs

DELEGATION_ONLY DNSKEY flag

Traditional Key Signing KEY DNSKEY record:

```
powerbind.nohats.ca.  IN DNSKEY 257 3 8 (
        AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
        ) ; KSK; alg = RSASHA256 ; key id = 17869

powerbind.nohats.ca.  IN DS 17869 8 2
f22bbb3315c48b719fb67da0fc019ae4af534143569f7a63022eba4d87c1f56d
```

DNSKEY with DELEGATION_ONLY flag set:

```
powerbind.nohats.ca.  IN DNSKEY 321 3 8 (
        AwEAAb+wQalXSsjykJ6uaIIGvHbzHZZDDeexZNCYJJBa
        ) ; KSK; alg = RSASHA256 ; key id = 17933

powerbind.nohats.ca.  IN DS 17933 8 2
096749AAB0CFE225A3779AC7BD21EBDC1D8573511DD5AFA0889EB5E8A00B9AF9
```

Does this break current deployment?

- powerbind.nohat.ca is a real signed zone using 0x40 DNSKEY flag
- used a patched dnssec-keygen to create key
- "ods-ksmutil key import" ignored my new dnskey flag
- dnssec-signzone worked
- So far all tested DNS resolves validate properly

Pros & Cons

- Protects child zone data from parent
  - Including TLSA, SMIMEA, OPENPGPKEY
- Allows DNSSEC Transparency
- Very simple
  - No new RRTYPE
  - no changes required for authoritative servers
  - Only minimal changes in validator

Pros & Cons

- Does not allow exceptions for ENT ("co.uk")
- Does not protect child APEX data
  - A/AAAA, MX, IPSECKEY[*]
- Requires adding delegations for _prefix labels
  e.g. for TLSA:
  _tcp.powerbind.nohats.ca IN NS …
  _tcp.powerbind.nohats.ca IN DS …