DNS-0x20

Use of Bit 0x20 in DNS Labels
to Improve Transaction Identity

Abstract

- 16-bit TXID + 14-bit ephemeral UDP port number = 30 bits = trivial to predict or guess
- Quality of one's PRNG does not really matter, birthday attacks worked even before Kaminsky
- Until we can get DNSSEC and SIG(0), or TKEY over TCP and TSIG for query, more bits needed
- There are some bits in the QNAME we can use, thanks to an idea by David Dagon of GATECH

Covert Channel in the QNAME

- If the value of a character cell in QNAME is from 0x41..0x5A (A..Z) or 0x61..0x7A (a..z), then the bit at 0x20 is not used by the responder
- Almost all responders will echo this bit back in its original form, not in the form held in cache or found in the zone
- Requestors can use this 0x20 bit as a covert channel to convey additional “nonce” bits from itself to itself via the authentic responder

0x20 Examples

- All of these are considered equivalent by DNS responders when they generate an answer:
  - `www.ietf.org`
  - `WWW.IETF.ORG`
  - `WwW.iEtF.oRg`
  - `wWw.IeTf.OrG`
- However, they are all different on the wire, and the difference can be useful to requestors

0x20 Bits

- Here are the 0x20 bits from the prior example:
  - `www.ietf.org  111 1111 111`
  - `WWW.IETF.ORG  000 0000 000`
  - `WwW.iEtF.oRg  010 1010 101`
  - `wWw.IeTf.OrG  101 0101 010`
- Thus a QNAME can longitudinally encode a random number whose length in bits is the number of [A-Za-z] characters in the QNAME

Responders Who Don't Copy

- All enhancements of this kind are subject to downgrade attacks, and some responders do not preserve the requestor's 0x20 bits
- In the event of a 0x20 mismatch, the requestor should try all other servers for that zone, trying each up to three times before giving up on 0x20
- This puts some stress on non-copying responders, which should incentivize them to start copying
- “Tough love”, yes, but it has a good endgame

Standardization Needs

- We are not asking that 0x20 processing become mandatory in requestors – it should be an available tool rather than a required method
- We are however asking that the DNS specs be amended to require that responders copy the entire QNAME including all 0x20 bits
- This is mostly moot, very few current responders fail to copy, but we want to reduce that to zero, and then keep it from growing