DNSSEC導入に伴うペイロード長の増加に関する研究の歴史と現状

力武 健次
NICT インシデント対策グループ
2009年11月24日 DNSOPS.JP BoF

DNSのペイロード長とは

DNSのメッセージの中身の長さ
- UDPではペイロードの長さと同じ
  UDPでは512バイト制限 (RFC1035 2.3.4)
  制限を超えるとTCビットが立って途中で切れる
  切れたパケットは不完全なのでTCPで要再送
- TCPだと2バイトのペイロード長が先に付く
  (RFC1035 4.2.2)

DNSSECでペイロードが大きくなる理由

RRSIG RRがすべてのRRにくっつく
- RRSIG自身とDNSKEY RRを除く
  1個あたり128バイト(1024bit)

DNSKEY RRのサイズ
- KSK: 4096bit → 514バイト
- ZSK: 1024bit → 130バイト
- メッセージあたりの署名以外のRRが同じなら,
  どう考えても512バイトには収まらない

DNSSECに対応したペイロード長

最低1220，できれば4000バイト
- RFC4035 Section 3

UDPではEDNS0必須 (RFC2671)

当然IP fragmentationの発生が前提
- 諸々の運用上の問題が発生する
  例1: ルータでfragmentが通らない
  例2: 偽造fragmentによる攻撃が可能
  例3: IPv6だとpath MTUの制限を受ける（後述）

ペイロード長問題に関する研究の歴史(1)

力武のやったこと
- IPv6で同じ問題に気づく (2002～2003)
- DNSSECはもっと大変なことに気づく (2005)
  最大パケット長が約4倍[1]
- DNSペイロードを使いIP fragmentがパス上通るかどうかの方法を開発[2](2007～2008)
  Mark Andrewsには「実装意味なし」と一蹴された

[1]Rikitake, K., Nogawa, H., Tanaka, T., Nakao, K. and Shimojo, S.: An Analysis of DNSSEC Transport Overhead Increase, *IPSJ SIG Technical Reports 2005-CSEC-28*, Vol. 2005, No. 33, pp. 345-350 (2005).
[2] Rikitake, K., Nakao, K., Shimojo, S. and Nogawa, H.: UDP Large-Payload Capability Detection for DNSSEC, *IEICE Trans. Inf. Sys.*, Vol. E91-D, No. 5, pp. 1261-1273 (2008).

ペイロード長問題に関する研究の歴史(2)

draft-ietf-dnsop-respsize
- Root Zoneのペイロード長に関する分析
- 2003～2008，-11でexpire

draft-barwood-dnsext-edns-page-option (2009年8月)
- UDPのIP fragmentationをなくすために，
  EDNS payloadの中に番号をつけて複数メッセージに分割

ペイロード長問題への視点: IETF76

Homegate BoF
- DNSSECのtrust anchorをGW箱に入れる
  自動設定の安全確保

dnsext WG
- DNS TCPトランスポートの必須化
  draft-ietf-dnsext-dns-tcp-requirements-01
- DNSに特化したTCPのチューニング?
- 結論は出ず

7

ペイロード長問題に関する現在の状況

EDNS0だけでは問題が解決しない
- GW箱（ルータ箱，NAT箱）の存在

DNSでTCPを義務化するかどうかの是非
- TCPにするとプロトコルスタックの負荷が増える
- HTTPでやっているのにDNSがダメな理由は?

そもそもGW箱の問題はプロトコル問題か?
- GW箱自身が対策すればいいのでは?
- 誰が対策するの?

8

今後の課題: IPv6 UDP fragmentation

IPv6：ルータでのfragmentationを禁止
- end pointでfragmentを作る必要がある

IPv6のpath MTU discoveryが不完全な場合，IP fragmentationが必要なUDPは通らない可能性がある
- end pointはMTUの変化を予測できない
- →DNSSECがIPv6では動かなくなる可能性
- 問題はDNSSECに限らない

9

個人的なまとめと雑感

正直言ってこれは研究じゃなくて開発
- DNSを実際にドップリ触れないと意味がない

研究にするなら大量のデータ解析が必要
- 目的意識を持たないと徒労感が非常に強い
- DNSの標準化は精神的胆力が必要

日本のオペレータの人達も動いて欲しい
- 長期的課題は日々の問題に必ずなります

10