IP フラグメンテーションを悪用したキャッシュポイズニング攻撃と対策

DNS Summer Day 2020

中京大学大学院 工学研究科 太田 健也

自己紹介

- 名前: 太田 健也
- 所属: 中京大学大学院 工学研究科
- 研究テーマ: キャッシュポイズニング
  - DNS 第一フラグメント便乗攻撃の追検証と対策の検討
  - A survey on the status of measures against IP fragmentation attacks on DNS

IP フラグメンテーションアタック

発表の流れ

- 攻撃概要
- アタックベクタ
- 対策
- TLD 対策状況の調査
- まとめ

攻撃概要

IP フラグメンテーションアタック

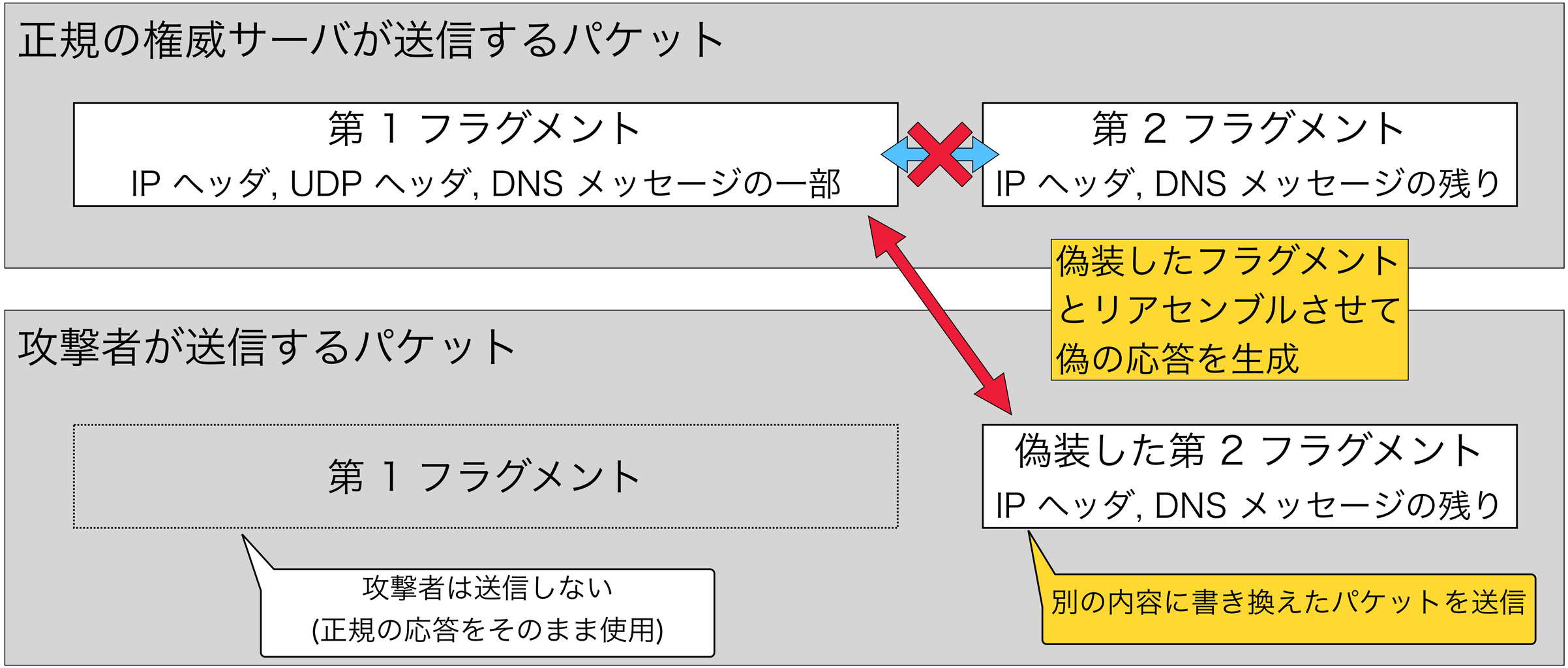
攻撃概要

- Herzberg, Shulman が 2012 年に論文発表
  - "Fragmentation Considered Poisonous" [1-3]
    - 第一フラグメント便乗攻撃とよばれることも
- フラグメントした 2 番目以降のパケットを偽物に差し替え
  - EDNS, DNSSEC などが影響
- Path MTU Discovery の偽装によりフラグメンテーションを誘発
  - RIPE 67 で Hlavacek が発表 [4]
    - 実際の Path MTU より小さいサイズでも攻撃可能
- ソースポートランダマイゼーションなどの対策は無効

[1] https://arxiv.org/abs/1205.4011
[2] https://u.cs.biu.ac.il/~herzbea/security/13-03-frag.pdf
[3] https://ieeexplore.ieee.org/document/6682711
[4] https://ripe67.ripe.net/presentations/240-ipfragattack.pdf

IP フラグメンテーションアタック

イメージ



IP フラグメンテーションアタック

応答例

正規の応答

guest@debian-ex1: ~ — ssh guest@192.168.56.101 — 111×35

```
; <<>> DiG 9.11.5-P1 <<>> @192.168.11.1 +dnssec +norec aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.a
aaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aa
aa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnssec.exp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9888
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.
aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnss
ec.exp. IN      A

;; AUTHORITY SECTION:
nodnssec.exp.           86400   IN      NS      ns1.nodnssec.exp.
nodnssec.exp.           86400   IN      NS      ns2.nodnssec.exp.
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN NSEC3 1 1 12 AABBCCDD HCO0EK0UJKBVUOO9846N8QOHO79QKCIP NS SOA RRSI
G DNSKEY NSEC3PARAM
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN RRSIG NSEC3 8 2 900 20301231235959 20180101000000 41979 exp. KeQYK
S1QTHKTav1gznMYxr7ngD6eG7F9J75gZ6OkHHJ0sxCHZDrY3zLy d/D2mQHP/BQEMxzOKFSdu7Nx8jIG/8mthd/CwErduq8ozYW9CecoLpSu tZ
yDMS0UzoPxsWCBcu3uBPGXo6LHgPUMFmqK0VECiBgHQ/tSy1EWuWdv 4OI=

;; ADDITIONAL SECTION:
ns1.nodnssec.exp.       86400   IN      A       192.168.11.7
ns2.nodnssec.exp.       86400   IN      A       192.168.11.8

;; Query time: 42 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Tue Jan 15 20:00:58 JST 2019
;; MSG SIZE  rcvd: 571

root@resolver:~ #
```

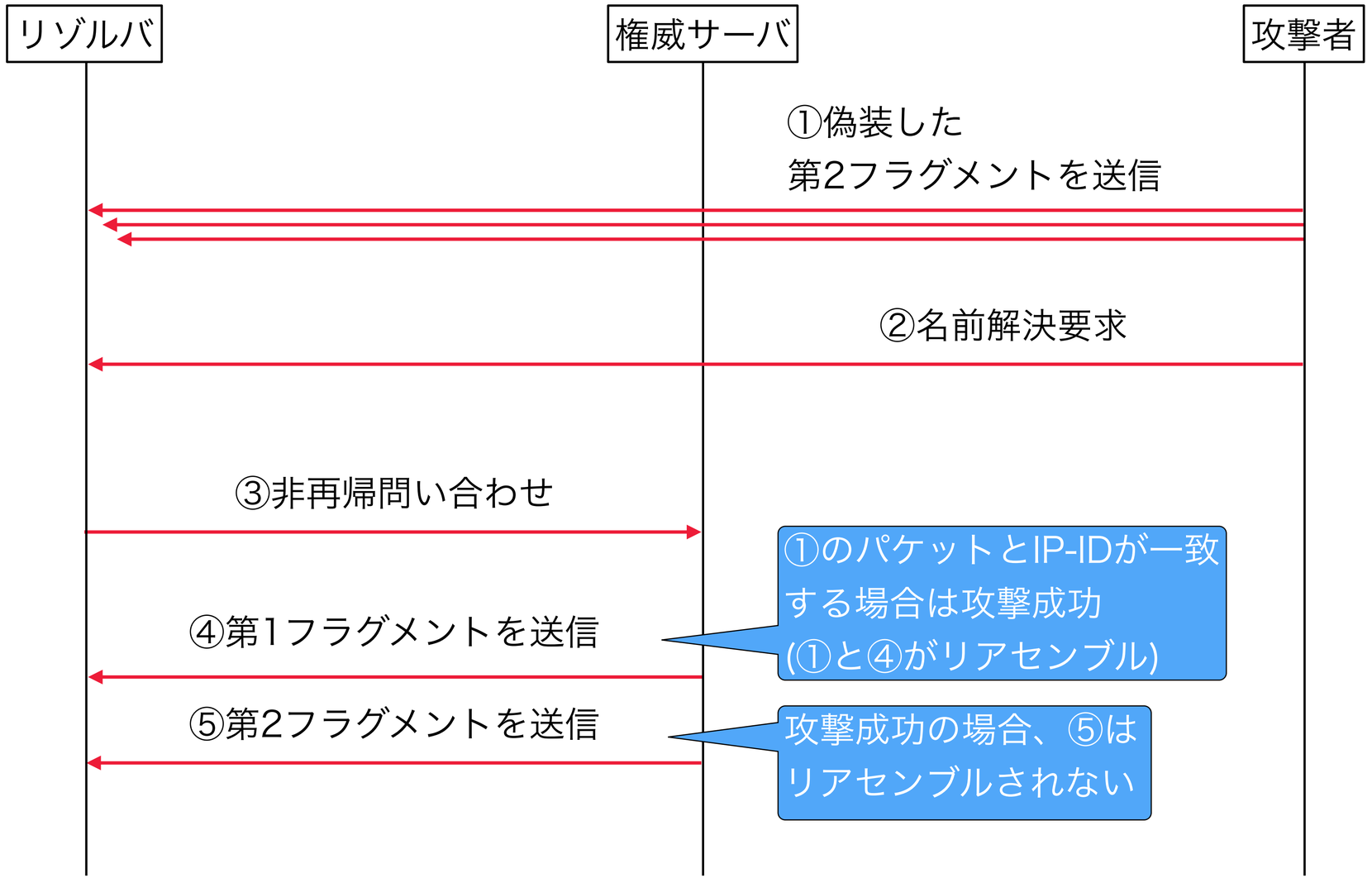
偽装した応答

guest@debian-ex1: ~ — ssh guest@192.168.56.101 — 111×35

```
; <<>> DiG 9.11.5-P1 <<>> @192.168.11.1 +dnssec +norec aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.a
aaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aa
aa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnssec.exp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53059
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.
aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnss
ec.exp. IN      A

;; AUTHORITY SECTION:
nodnssec.exp.           86400   IN      NS      ns1.nodnssec.exp.
nodnssec.exp.           86400   IN      NS      ns2.nodnssec.exp.
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN NSEC3 1 1 12 AABBCCDD HCO0EK0UJKBVUOO9846N8QOHO79QKCIP NS SOA RRSI
G DNSKEY NSEC3PARAM
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN RRSIG NSEC3 8 2 900 20301231235959 20180101000000 41979 exp. KeQYK
S1QTHKTav1gznMYxr7ngD6eG7F9J75gZ6OkHHJ0sxCHZDrY3zLy d/D2mQHP/BQEMxzOKFSdu7Nx8jIG/8mthd/CwErduq8ozYW9CecoLpSu tZ
yDMS0UzoPxsWCBcu3uBPGXo6LHgPUMFmqK0VECiBgHQ/tSy1EWuWdv 4OI=

;; ADDITIONAL SECTION:
ns1.nodnssec.exp.       86400   IN      A       192.168.13.1
ns2.nodnssec.exp.       85389   IN      A       192.168.13.1

;; Query time: 39 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Tue Jan 15 20:01:48 JST 2019
;; MSG SIZE  rcvd: 571

root@resolver:~ #
```

IP フラグメンテーションアタック

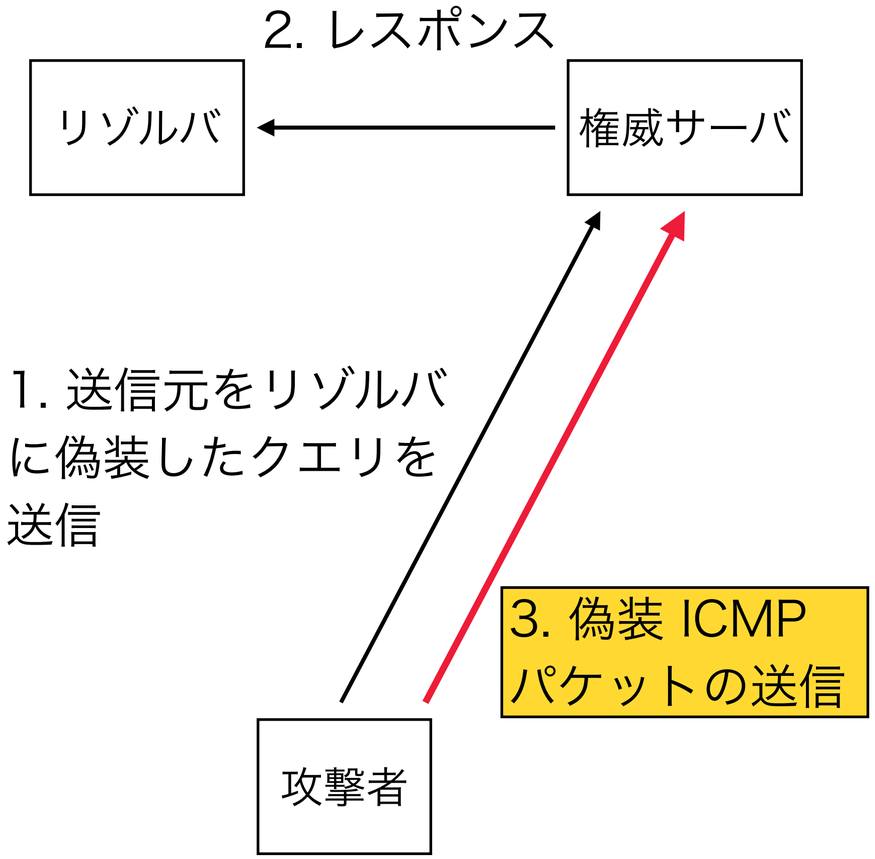
攻撃手順



攻撃のポイント

Path MTU Discovery

- 経路上の MTU を探索し、送信元でフラグメント
  - 経路途中でのフラグメンテーションを抑制
  - IPv6 では経路途中のフラグメンテーションは行わない
- 外部から偽装した ICMP パケットを送信可能
  - IPv4 における影響
    - Linux: あり (Kernel 5.6.5 で確認)
    - FreeBSD 12.0: なし



攻撃のポイント

MTU とフラグメント位置

- MTU
  - IPv4 は 68 バイト以上、IPv6 は 1280 バイト以上
  - Linux カーネルデフォルトの IPv4 Path MTU 最小値は 552 バイト
- IP のペイロード (UDP ヘッダの位置) から 8 バイト単位でフラグメント
  - Path MTU が 552 バイトなら 548 バイトのパケットが送信
- qname で微調整

攻撃のポイント

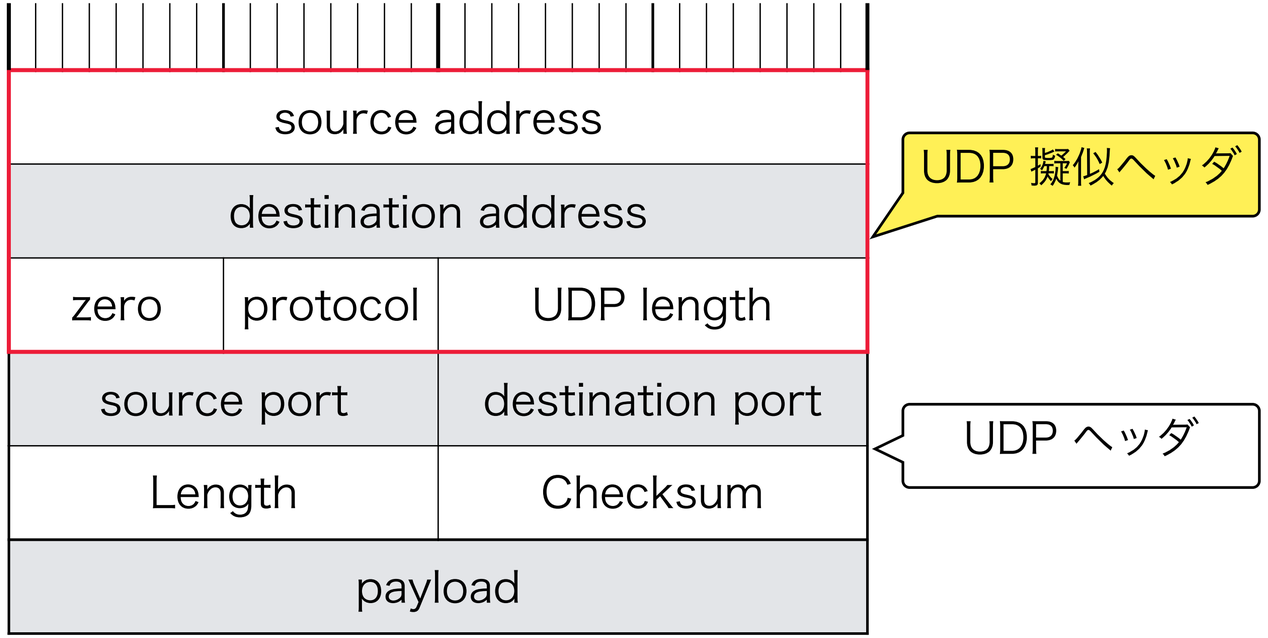
フラグメントパケットの偽装

- UDP ヘッダ、DNS Header セクションは最初のフラグメントに存在
  - ソースポートや TXID は変更できない
  - 最初のフラグメントは正規のものを使用するため無視できる
    - ソースポートランダマイゼーションや TXID ランダマイゼーションは無効
- 主に次の項目の整合性をとる
  - UDP チェックサム
  - IP Identification
  - 各セクションの RR 数

攻撃のポイント

UDP チェックサム

- UDP 擬似ヘッダ、UDP ヘッダ、ペイロードから計算
- 2 バイトずつ順に加算して 1 の補数和の 1 の補数を求める
  - バイト長が奇数なら偶数になるようにゼロパディング
  - 繰り上がり分は最下位ビットに加算



攻撃のポイント

UDP チェックサムの偽装

- クエリごとにチェックサムは変化
- 応答内容とフラグメント位置が不変なら、２番目以降のフラグメントのペイロードは不変
- フラグメントごとに補数和の計算が一致すればよい
- ２バイトのフィールドがあれば調整可能
  - TTL を操作
- あらかじめ正規の応答を用意して偽装ペイロードを調整

$Csum = Csum_1 + Csum_2$

$Csum' = Csum_1 + Csum_2'$

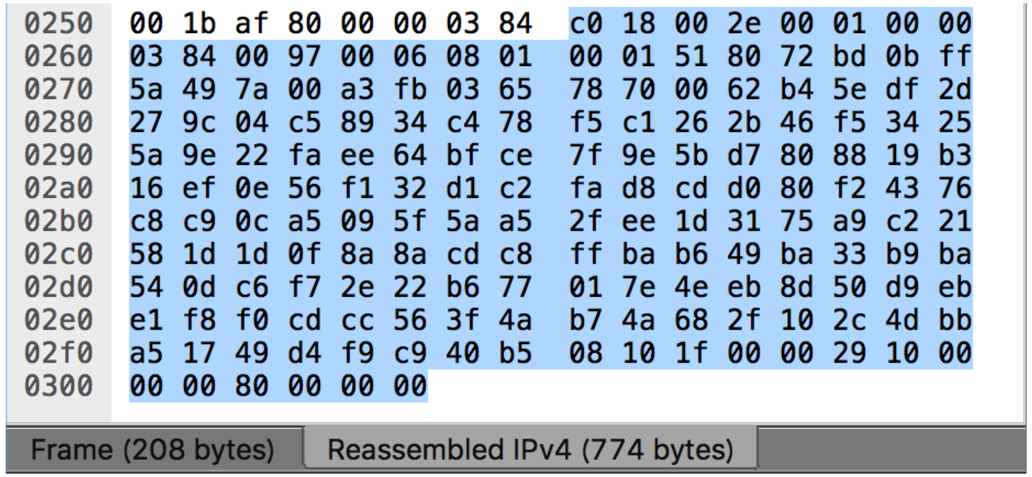
$Csum_2 = Csum_2'$ ならば $Csum = Csum'$

($Csum$：1 の補数和)

攻撃のポイント

UDP チェックサムの偽装

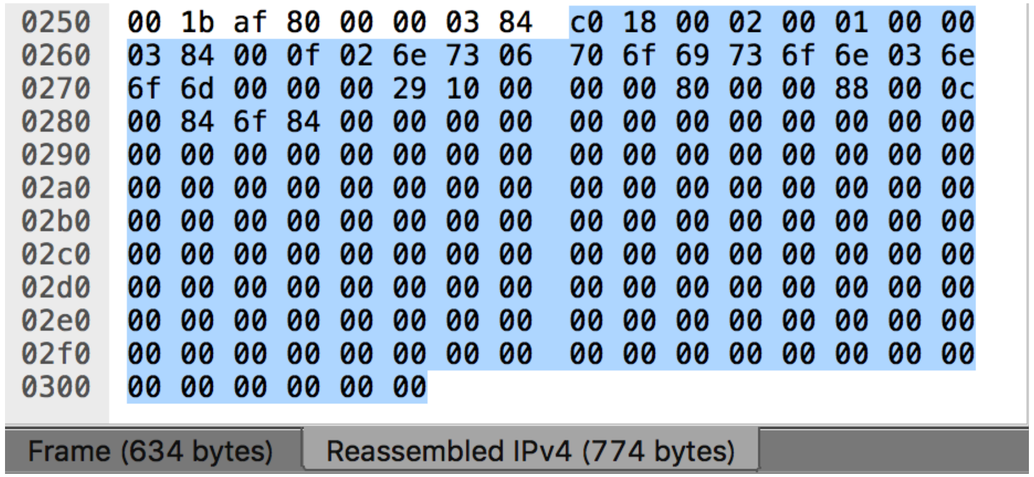
正規応答の例



2 バイトずつ加算した合計値: `0x22F5F3`

1 の補数和: `0xF615`

偽装応答の例



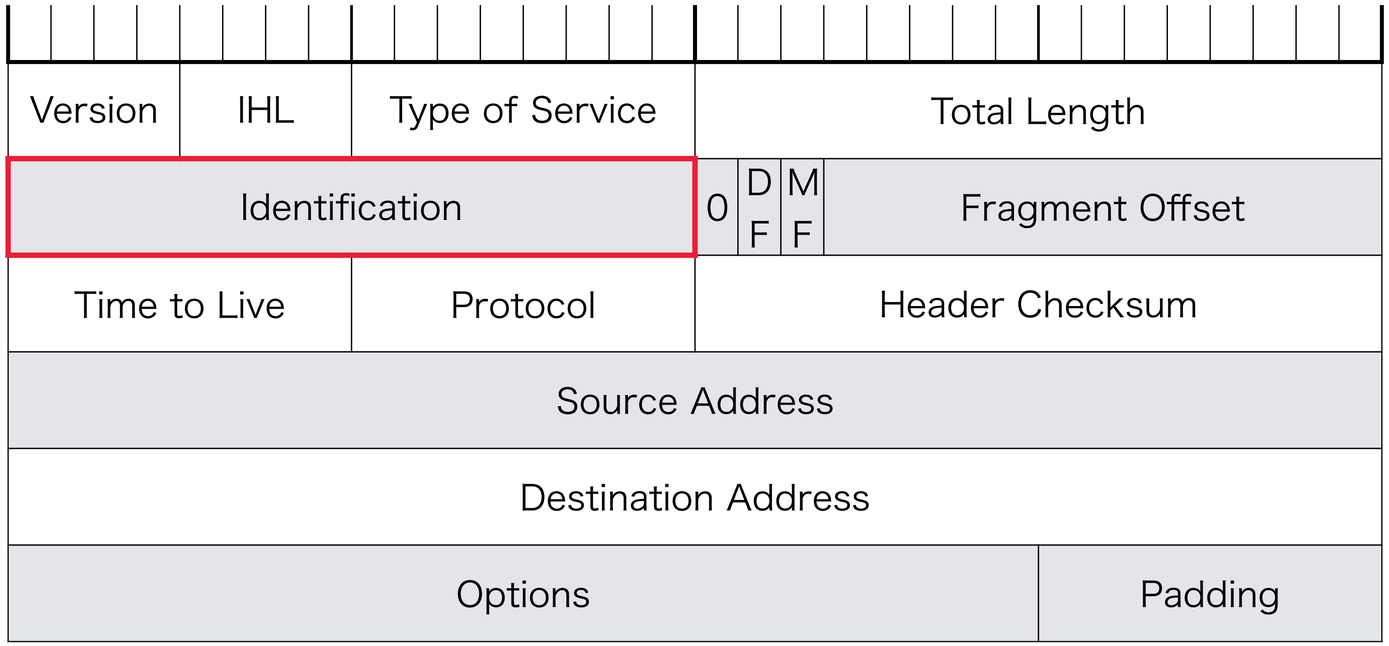
2 バイトずつ加算した合計値: `0x3F612`

1 の補数和: `0xF615`

攻撃のポイント

IP Identification

- IPv4: 16 ビット
- 決定方法は実装依存
- 攻撃者が予測する必要がある



IPv4 ヘッダ

アタックベクタ

アタックベクタ

攻撃例

- 委譲応答の差し替え
- sibling domain の glue レコードの差し替え
- 否定応答の差し替え

アタックベクタ

委譲応答の差し替え

- 署名ゾーンから未署名ゾーンへの委譲応答を攻撃
  - 署名検証有効時でも攻撃可能なケースも
    - NSEC3 Opt-Out が有効なゾーンの Opt-Out 区間への委譲
    - 署名ツールに依存
- 対象ゾーンがキャッシュに存在しない場合に有効
- 大量の NS を持つ場合や NS のラベルが長い場合はより危険
  - NSEC3/RRSIG がなくてもフラグメントさせられる可能性

アタックベクタ

委譲応答の差し替え

guest@debian-ex1: ~ — ssh guest@192.168.56.101 — 111×35

```
; <<>> DiG 9.11.5-P1 <<>> @192.168.11.1 +dnssec +norec aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.a
aaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aa
aa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnssec.exp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9888
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.
aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.nodnss
ec.exp. IN      A

;; AUTHORITY SECTION:
nodnssec.exp.           86400   IN      NS      ns1.nodnssec.exp.
nodnssec.exp.           86400   IN      NS      ns2.nodnssec.exp.
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN NSEC3 1 1 12 AABBCCDD HCO0EK0UJKBVUO09846N8QOHO79QKCIP NS SOA RRSI
G DNSKEY NSEC3PARAM
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN RRSIG NSEC3 8 2 900 20301231235959 20180101000000 41979 exp. KeQYK
S1QTHKTav1gznMYxr7ngD6eG7F9J75gZ6OkHHJ0sxCHZDrY3zLy d/D2mQHP/BQEMxzOKFSdu7Nx8jIG/8mthd/CwErduq8ozYW9CecoLpSu tZ
yDMS0UzoPxsWCBcu3uBPGXo6LHgPUMFmqK0VECiBgHQ/tSy1EWuWdv 40I=

;; ADDITIONAL SECTION:
ns1.nodnssec.exp.       86400   IN      A       192.168.11.7
ns2.nodnssec.exp.       86400   IN      A       192.168.11.8

;; Query time: 42 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Tue Jan 15 20:00:58 JST 2019
;; MSG SIZE  rcvd: 571

root@resolver:~ #
```

差し替え対象のレコード

```
;; ADDITIONAL SECTION:
ns1.nodnssec.exp.       86400   IN      A       192.168.11.7
ns2.nodnssec.exp.       86400   IN      A       192.168.11.8

;; Query time: 42 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Tue Jan 15 20:00:58 JST 2019
;; MSG SIZE  rcvd: 571
```

正規応答

IPアドレスの置きかえ

```
;; ADDITIONAL SECTION:
ns1.nodnssec.exp.       86400   IN      A       192.168.13.1
ns2.nodnssec.exp.       85389   IN      A       192.168.13.1

;; Query time: 39 msec
;; SERVER: 192.168.11.1#
;; WHEN: Tue Jan 15 20:0
;; MSG SIZE  rcvd: 571
```

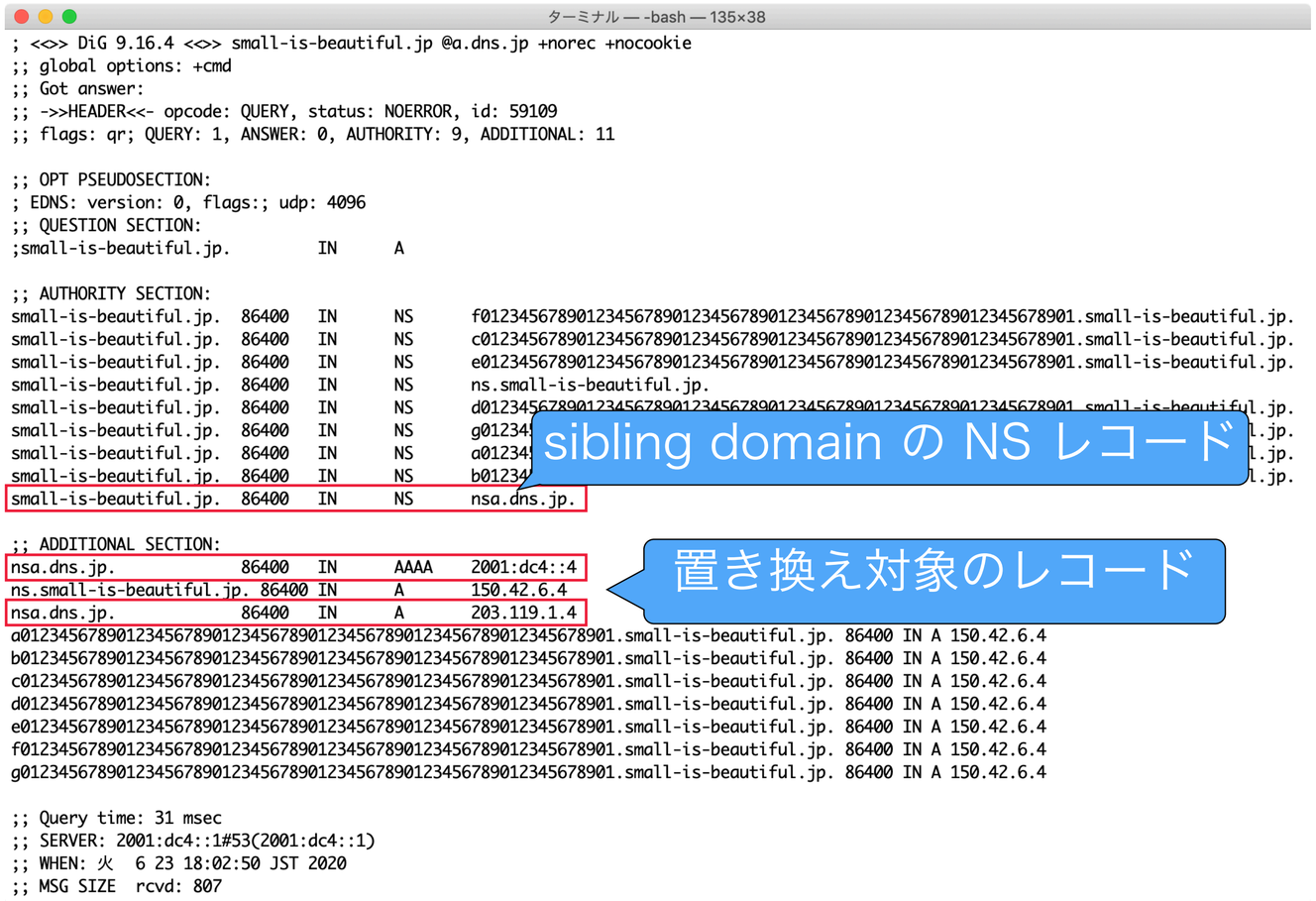
TTLによる
チェックサムの調整

偽装応答

アタックベクタ

sibling domain の glue レコードの差し替え

- 攻撃者自身がドメイン名を用意
  - sibling domain の NS に委譲しているようにみせかけ
  - Additional セクションの A/AAAA レコードを偽装
- 偽装するレコードがキャッシュされている場合に上書き可能かどうかは実装依存



アタックベクタ

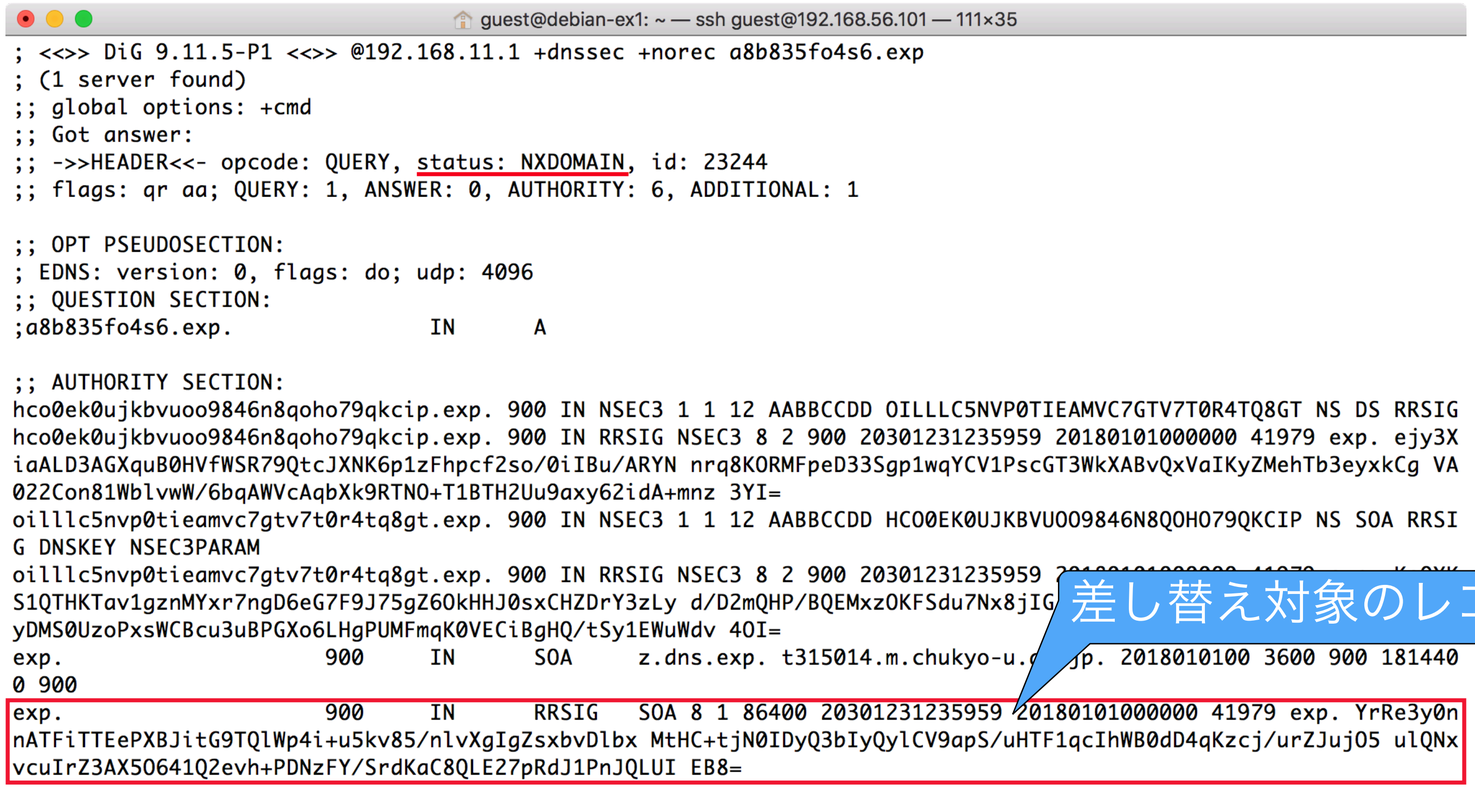
否定応答の差し替え

- メジャーな OSS 実装は対策済み
  - BIND, Knot Resolver は影響なし (BIND 9.11.5-P1, Knot Resolver 3.1.0 で確認)
  - Unbound 1.8.2 [5], PowerDNS Recursor 4.2.0 [6] で修正
- 署名ゾーンへ DO ビットをオンにして問い合わせる場合を想定
- 影響
  - 署名未検証: ドメインハイジャック
  - 署名検証時: NSEC3 Opt-Out 区間へサブドメインインジェクションできる可能性
- 連続攻撃が可能

[5] https://www.nlnetlabs.nl/news/2018/Dec/04/unbound-1.8.2-released/
[6] https://github.com/PowerDNS/pdns/pull/7258

アタックベクタ

否定応答の差し替え



正規応答

アタックベクタ

否定応答の差し替え

guest@debian-ex1: ~ — ssh guest@192.168.56.101 — 111×35

```
; <<>> DiG 9.11.5-P1 <<>> @192.168.11.1 +dnssec +norec a8b835fo4s6.exp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 13347
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; PAD: 6f 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ("o.....
.....................................................................................")
;; QUESTION SECTION:
;a8b835fo4s6.exp.               IN      A

;; AUTHORITY SECTION:
hco0ek0ujkbvuoo9846n8qoho79qkcip.exp. 900 IN NSEC3 1 1 12 AABBCCDD OILLLC5NVP0TIEAMVC7GTV7T0R4TQ8GT NS DS RRSIG
hco0ek0ujkbvuoo9846n8qoho79qkcip.exp. 900 IN RRSIG NSEC3 8 2 900 20301231235959 20180101000000 41979 exp. ejy3X
iaALD3AGXquB0HVfWSR79QtcJXNK6p1zFhpcf2so/0iIBu/ARYN nrq8KORMFpeD33Sgp1wqYCV1PscGT3WkXABvQxVaIKyZMehTb3eyxkCg VA
022Con81WblvwW/6bqAWVcAqbXk9RTNO+T1BTH2Uu9axy62idA+mnz 3YI=
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN NSEC3 1 1 12 AABBCCDD HCO0EK0UJKBVUOO9846N8QOHO79QKCIP NS SOA RRSI
G DNSKEY NSEC3PARAM
oilllc5nvp0tieamvc7gtv7t0r4tq8gt.exp. 900 IN RRSIG NSEC3 8 2 900 20301231235959 20180101000000 41979 exp. KeQYK
S1QTHKTav1gznMYxr7ngD6eG7F9J75gZ6OkHHJ0sxCHZDrY3zLy d/D2mQHP/BQEMxzOKFSdu7Nx8jIG/8mthd/CwErduq8ozYW9CecoLpSu tZ
yDMS0UzoPxsWCBcu3uBPGXo6LHgPUMFmqK0VECiBgHQ/tSy1EWuWdv 4OI=
exp.                    900     IN      SOA     z.dns.exp. t315014.m.chukyo-u.ac.jp. 2018010100 3600 900 181440
0 900
exp.                    900     IN      NS      ns.poison.nom.

;; Query time: 26 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Tue Jan 15 19:50:17 JST 2019
;; MSG SIZE  rcvd: 766
```

EDNS パディングオプションによる
メッセージサイズとチェックサムの調整

差し替え後のレコード

偽装応答

対策

対策

権威・リゾルバ双方の対策

- 完璧な対策は困難
  - MTU の小さい経路での副作用が心配
- EDNS buffer size を小さくする
  - 指定したサイズより大きい応答は TCP フォールバック
  - DNS flag day 2020 では 1232 バイトを推奨
    - より小さいサイズでフラグメントする可能性
  - 筆者らは 512 バイトを推奨
    - Linux における Path MTU の偽装を考慮
    - パフォーマンスに影響

対策

権威・リゾルバ双方の対策

- DNSSEC への"完全な"対応
  - NSEC3 Opt-Out も無効に
  - 普及途上が危険
    - リゾルバの DO ビットが有効だと未署名ゾーンへの委譲応答に NSEC3/RRSIG が付加
    - Shulman ら [1] の指摘

> *"incremental DNSSEC deployment is vulnerable to our cache poisoning attacks, and complete adoption of DNSSEC may take considerable time, since it depends on adoption by both name server and resolver."*

対策

権威側

- PMTUD の結果を無視
  - Linux Kernel 3.15 以降の `IP_PMTUDISC_OMIT` ソケットオプションを有効に
  - OS と権威サーバ実装両方の対応が必要
    - BIND 9.9.10/9.10.5/9.11.1 以降 [7]
    - NSD 4.1.27 以降 [8]
    - Knot DNS 2.8.2 以降 [9]
    - PowerDNS 4.2.0-rc2 以降 [10]

[7] https://www.isc.org/blogs/bind-april-2017/
[8] https://www.nlnetlabs.nl/projects/nsd/download/#nsd-4-1-27
[9] https://www.knot-dns.cz/2019-06-05-version-282.html
[10] https://doc.powerdns.com/authoritative/changelog/4.2.html#change-4.2.0-rc2

対策

リゾルバ側

- フラグメントした UDP パケットをドロップ
- 署名検証しない場合は DO ビットをオフに
  - RRSIG や NSEC3 は不要
  - メッセージサイズを削減

対策

その他の緩和策

- QNAME minimisation
  - Empty Non-Terminal など副作用あり
- 各ゾーンの NS + A/AAAA レコードを Authoritative Answer としてキャッシュ
  - より高い信頼度の応答を得る
    - RFC 2181 section 5.4.1 Ranking data
  - キャッシュの上書きを防止

TLD 対策状況の調査

調査

TLD の対策状況

- 対象: 2019 年 8 月時点でルートゾーンに DS が登録されている TLD
  - IPv4 のみ調査
- 調査期間: 2019 年 8 月、10 月
- 調査内容
  - PMTUD により以下の応答がフラグメントするかどうか
    - ICMP の echo reply
    - NXDOMAIN になるドメイン名の問い合わせ
  - EDNS buffer size の設定値

調査

TLD と権威サーバの変化

- 8 月: 1387 ドメイン
  - 合計 3151 アドレスの権威サーバ
- 10 月: 1384 ドメイン
  - 合計 3127 アドレスの権威サーバ
- IP アドレスの変化
  - 減少: 44 アドレス
  - 増加: 20 アドレス

調査

IP アドレスごとのスキャン結果

- ICMP フラグメンテーション
  - 8 月: 2123 (=1792+328+3) アドレス (67.4%) がフラグメント
  - 10月: 2096 (=1759+334+3) アドレス (67.0%) がフラグメント
  - フラグメントした際のパケットサイズはすべて 548 バイト

	DNS fragmentation					
	2019/08			2019/10		
ICMP frag	Yes	No	noreply	Yes	No	noreply
Yes	1792	328	3	1759	334	3
No	52	896	0	52	902	1
noreply	0	75	5	0	71	5

調査

IP アドレスごとのスキャン結果

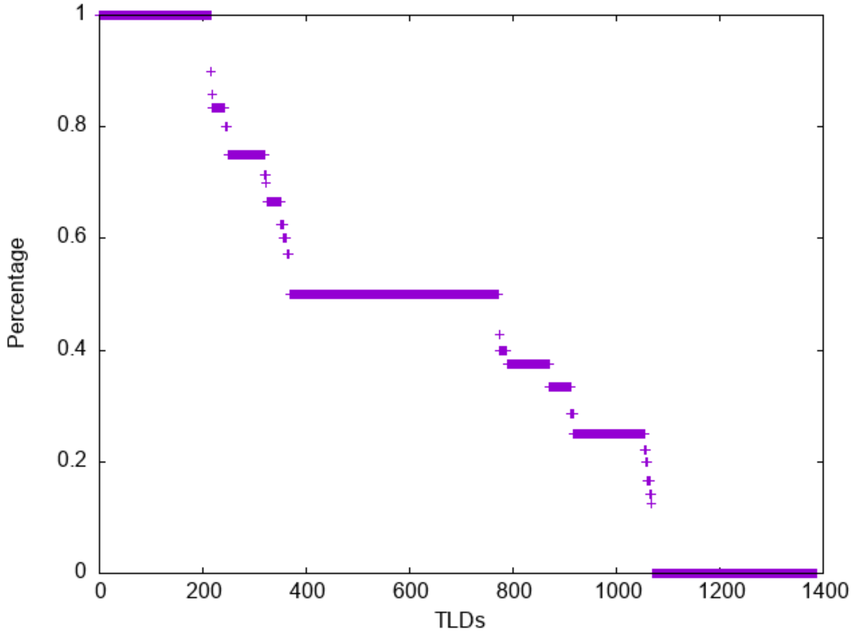
- DNS フラグメンテーション
  - 8 月: 1844 (=1792+52+0) アドレス (58.5%) がフラグメント
  - 10月: 1811(=1759+42+0) アドレス (57.9%) がフラグメント

	DNS fragmentation					
	2019/08			2019/10		
ICMP frag	Yes	No	noreply	Yes	No	noreply
Yes	1792	328	3	1759	334	3
No	52	896	0	52	902	1
noreply	0	75	5	0	71	5

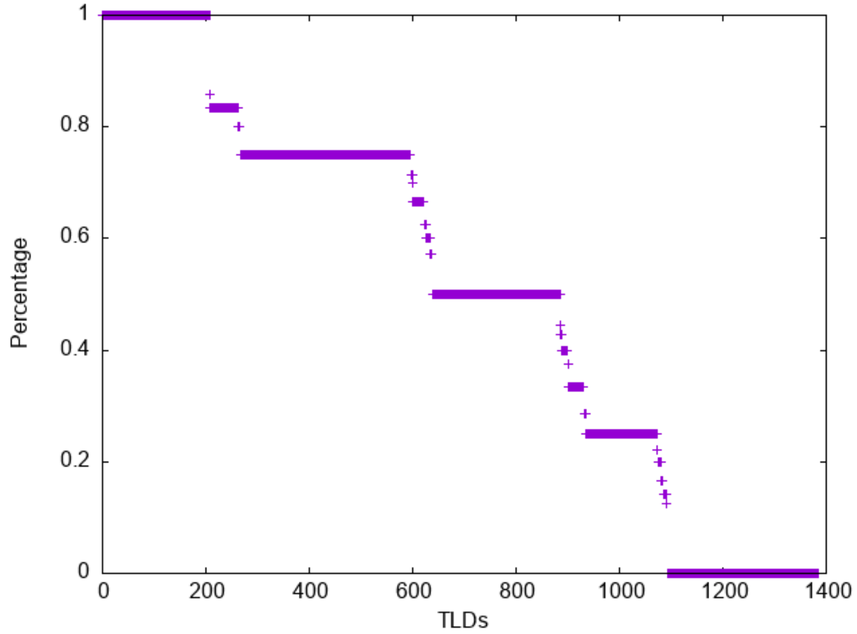
調査

TLD ごとの DNS 応答のフラグメント結果

- 各 TLD の全 NS にしめるフラグメント応答を返す NS の割合
  - 過半数の TLD がフラグメント応答を返す NS を半数以上使用
    - 8 月は 55.7%、10 月は 64.0% が該当



2019/08



2019/10

調査

EDNS buffer size の設定

- 4096 バイトが最多
  - buffer size の削減は進んでいない

	count			
	2019/08		2019/10	
bufsize	all	frag	all	frag
512	35	0	35	0
1220	15	0	15	0
1232	30	0	65	0
1280	20	5	20	5
1432	18	10	15	10
1450	5	1	5	1
1472	3	0	2	0
1480	5	0	5	0
1680	5	5	5	5
4096	15540	5663	15393	5619
32768	5	0	5	0

まとめ

IP フラグメンテーションアタック

まとめ

- IP フラグメンテーションしたパケットの一部を差し替える攻撃
- アタックベクタ、実装により影響は変化
- EDNS buffer size を小さくする、フラグメントパケットをドロップする

  などの対策

  - TCP 対応は必須