4ZA-04

DNS 第一フラグメント便乗攻撃の追検証と対策の検討

太田　健也†　　鈴木　常彦†
†中京大学工学部情報工学科

1　はじめに

DNS キャッシュポイズニングの対策として導入された DNSSEC では，リソースレコード集合に対する電子署名などを応答に含むため，DNS メッセージサイズが増大する．また，DNSSEC で対応を必須としている EDNS により，512 バイトを超える応答を UDP で扱えるようになったほか，多くのリゾルバ実装が署名検証実施の有無によらず，デフォルトで DO ビットをオンにして名前解決を行う．そのため，応答時に IP フラグメントが生じる可能性が高まっている．

それに伴い，Shulman らは IP フラグメントを差し替えることでキャッシュポイズニングを試みる第一フラグメント便乗攻撃の危険性を指摘した [1]．しかし，攻撃検証コードが公開されておらず，影響の評価や対策の検討が不十分である．そのため，本研究では主要なオープンソースのリゾルバ実装において本攻撃が可能かどうかを追検証し，影響の評価と対策の検討を行った．

2　第一フラグメント便乗攻撃

第一フラグメント便乗攻撃は IP フラグメントのリアセンブル処理を悪用する．UDP 通信時にフラグメントが生じる場合，最初のフラグメント以外には DNS メッセージを同定するための情報が含まれないため，フラグメントの差し替えによる応答の改竄が可能である．攻撃の影響は実装やキャッシュの状況により異なる．

攻撃要件として，IP Identification (IP-ID) などの IP ヘッダの情報のほか，UDP チェックサムなどの UDP ヘッダの情報，DNS メッセージの各セクションのレコード数などが正規の応答と一致する必要がある．UDP チェックサムは，正規の応答内容が変化しない限り，レコードの TTL や EDNS のパディングオプションによる調整を行うことで一致させることができる．また，Linux では Path MTU Discovery (PMTUD) により外部から MTU を調整可能であることを Hlaváček が示しており [2]，OS 実装によってフラグメント位置の調整が可能であると考えられ，今回その実在も確認した．

3　攻撃検証

本研究では，Shulman らが示した手法のうち，DNSSEC 署名されたゾーンからの否定応答に含まれる RRSIG レコードを NS レコードに差し替える方法と，Hlaváček が示した委譲応答の A レコードを差し替える方法を再現し，攻撃の検証を行った．

否定応答差し替え攻撃では，RFC 2181 で規定されている DNS Ranking に基づき，委譲応答で得た NS レコードを否定応答の Authority セクションに含まれる NS レコードで上書きできる可能性があることを悪用する．否定応答について規定した RFC 2308 ではこの形式が例示されており，これらに準拠した実装では攻撃が成功すると予想される．

委譲応答差し替え攻撃では，署名されたゾーンから未署名のゾーンへの委譲応答を攻撃対象とした．この攻撃では，委譲時の NS レコードや A レコードに RRSIG レコードが存在しないことと，未署名ゾーンは DNSSEC で保護されないことを悪用する．そのため，この攻撃は署名検証を行うリゾルバに対しても有効であることが予想される．

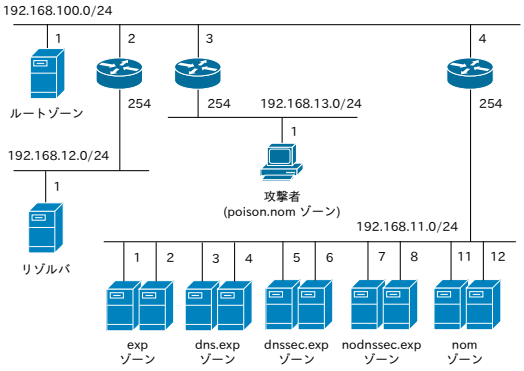

図 1: 検証環境

3.1　検証対象

検証対象のリゾルバ実装は BIND 9.11.5-P1，Unbound 1.8.1，Knot Resolver 3.1.0，PowerDNS Recursor 4.1.8 の 4 種類とし，否定応答差し替え攻撃では，筆者らの指摘により否定応答中の NS レコードを無視する対策が取られた Unbound 1.8.3 についても検証を行った．検証時はオープンリゾルバの状態とし，署名検証の設定を切り替えて挙動を検証した．Unbound では minimal-response と QNAME Minimisation を無効にして検証を行った．

3.2　検証環境

検証環境を図 1 に示す．VirtualBox 上の仮想マシンとして FreeBSD 11.2 および Debian 9.6 を用意し，VirtualBox の内部ネットワークと FreeBSD の仮想化機能である jail，VIMAGE を用いて権威サーバ，リゾルバ，攻撃者ホストからなる検証環境を構築した．権威サーバには NSD 4.1.14，署名ツールは dnssec-signzone 9.10.3-P4 を使用した．各リゾルバは FreeBSD 上で実行した．

仮想の名前空間として，DNSSEC 署名したルートゾーン，NSEC3 Opt-Out フラグをオンにして署名した exp ゾーンと dnssec.exp ゾーン，署名していない dns.exp ゾーン，nodnssec.exp ゾーン，root-servers.nom ゾーン，poison.nom ゾーンを用意した．exp 以下の各ゾーンと nom ゾーンは Debian 上の NSD，その他のゾーンは FreeBSD 上の NSD でホストした．

exp ゾーンには dnssec.exp ゾーンの DS レコードを登録し，NSEC3 レコード生成時の salt は aabbccdd，ハッシュ回数は 12 回として署名を行った．

poison.nom ゾーンは攻撃者が管理するゾーンとし，偽装した exp ゾーンと nodnssec.exp ゾーンを同居する．

3.3　検証手順

キャッシュに存在する攻撃対象ゾーンのレコードを削除した状態で以下の攻撃を複数回実行し，挙動を検証した．攻撃後の挙動はリゾルバに対して存在しないドメイン名を問い合わせることで確認し，一度でも偽の A レコードを応答した場合は攻撃が成功したとみなす．署名検証有効時は DO ビットをオンにし，CD ビッ

A proof of concept and countermeasures for 1st-fragment piggybacking attacks
Kenya OTA†　Tsunehiko SUZUKI†
†School of Engineering, Chukyo University

トを切り替えてリゾルバへの問い合わせを行った．また，キャッシュダンプが可能な実装ではキャッシュの内容も確認した．

3.3.1 否定応答差し替え攻撃

exp ゾーンの権威サーバに対し，PMTUD によりリゾルバまでの MTU を 620 バイトに設定して以下の手順を 10 分間繰り返す．IP-ID は未知であるとする．

1. exp ゾーンに対し，否定応答の Authority セクションのレコード数が 6 個になるようなドメイン名を問い合わせ，その応答を攻撃に使用する．
2. 応答の Authority セクションの最後の RRSIG レコードを ns.poison.nom を指す NS レコードに差し替え，UDP チェックサムとペイロード長が一致するように EDNS のパディングオプションによる調整を行う．
3. 偽装パケットの送信元を権威サーバ，宛先をリゾルバとし，IP-ID を変化させながらリゾルバへ送信する．
4. リゾルバに対し，1 を満たすドメイン名を問い合わせる．

3.3.2 委譲応答差し替え攻撃

exp ゾーンの権威サーバに対し，PMTUD によりリゾルバまでの MTU を 556 バイトに設定して以下の手順を一度実行する．IP-ID は既知であるとする．

1. exp ゾーンに対し，DNS メッセージの内部表現で 229 バイトになる nodnssec.exp ゾーンの存在しないドメイン名を問い合わせ，その応答を攻撃に使用する．
2. 応答の Additional セクション中の A レコードの RDATA を 192.168.13.1 に置きかえ，UDP チェックサムが一致するように 2 個目の A レコードの TTL の調整を行う．
3. 偽装パケットの送信元を権威サーバ，宛先をリゾルバとし，IP-ID を変化させながらリゾルバへ送信する．
4. リゾルバに対し，1 を満たすドメイン名を問い合わせる．

3.4 検証結果

否定応答差し替え攻撃後の挙動を表 1 に示す．Unbound 1.8.1 と PowerDNS Recursor では攻撃が成功し，署名検証が有効な場合であっても CD ビットをオンにすることで偽装レコードを応答した．Unbound 1.8.1 では，CD ビットがオフの場合でも偽装応答を返すことがあった．否定応答中の NS レコードを無視する BIND や Unbound 1.8.3，Knot Resolver では攻撃が失敗した．

委譲応答差し替え攻撃後の挙動を表 2 に示す．BIND と Unbound では条件によらず攻撃が成功した．PowerDNS Recursor では特定条件下で攻撃が成功することを観測した．Knot Resolver は QNAME Minimisation による問い合わせを行い，署名検証無効時に DO ビットをオフにするため攻撃が失敗した．

挙動確認の際，PowerDNS では攻撃が成功したときであっても場合により正規の応答を返すことがあった．

表 1: 否定応答差し替え攻撃後の挙動

実装	署名検証	攻撃後の挙動
BIND	有効	NXDOMAIN
	無効	NXDOMAIN
Unbound 1.8.1	有効	SERVFAIL / Answer (CD ビットオンの際 Answer)
	無効	Answer
Unbound 1.8.3	有効	NXDOMAIN
	無効	NXDOMAIN
Knot Resolver	有効	NXDOMAIN
	無効	NXDOMAIN
PowerDNS Recursor	有効	SERVFAIL (CD ビットオンの際 Answer)
	無効	Answer

表 2: 委譲応答差し替え攻撃後の挙動

実装	署名検証	攻撃後の挙動
BIND	有効	Answer
	無効	Answer
Unbound	有効	Answer
	無効	Answer
Knot Resolver	有効	NXDOMAIN
	無効	NXDOMAIN
PowerDNS Recursor	有効	NXDOMAIN (特定条件下で Answer)
	無効	Answer

4 対策

本攻撃の根本的な対策として，EDNS バッファサイズを 512 バイトに設定し，それを超える応答は TCP にフォールバックしてフラグメント差し替えを困難にすることが有効である．また，署名検証を行わない場合は DO ビットをオフにしてメッセージサイズを削減し，アタックベクタを限定することも緩和策として考えられる．さらに，各ゾーンに対してそのゾーンの NS レコードを問い合わせ，DNS Ranking に基づく信頼度の高い応答としてレコードをキャッシュすることで，NS レコードの上書きを困難にできる可能性がある．

Unbound 1.8.2 以降に導入された否定応答中の NS レコードを無視する対策は，否定応答差し替え攻撃に対して有効である．また，委譲応答差し替え攻撃に対しては，QNAME Minimisation による問い合わせ名の削減を行うことが緩和策として考えられる．

RFC 7873 で規定されている DNS Cookies は，Cookie が存在するフラグメントの差し替えを困難にするが，その他のフラグメントはペイロードを予測可能なため十分な対策とはならない．

DNSSEC への完全な対応により本攻撃への対策が可能であると考えられるが，運用が困難，サーバの負荷が高くなるなどの課題がある．そのため，すべてのゾーンが署名を行うようになるのは非現実的であり，その普及途上こそが危険であるといえる．

5 まとめ

本研究では，第一フラグメント便乗攻撃の追検証を行い，対策を検討した．検証結果より，本攻撃が可能であることと，実装やアタックベクタにより影響が異なることがわかった．対策手法として，EDNS バッファサイズを調整することや，DO ビットをオフにして IP フラグメントの発生を抑制することなどが考えられる．

今後の課題として，OS 毎の IP-ID の決定方法や IP フラグメントのリアセンブル処理，PMTUD の処理の実装差による攻撃への影響を評価することが挙げられる．また，本攻撃に未知のアタックベクタが存在しないか検討し，必要に応じて追加の評価を行うことが考えられる．

参考文献

[1] Amir Herzberg and Haya Shulman, “Fragmentation Considered Poisonous,” https://u.cs.biu.ac.il/~herzbea/security/13-03-frag.pdf, 2013.

[2] Tomáš Hlaváček, “IP fragmentation attack on DNS,” https://ripe67.ripe.net/presentations/240-ipfragattack.pdf, 2013.