第21部

DNS extension and operation environment

石原 知洋

第１章　はじめに

DNS WGでは、DNSにおける実装上や運用上の問題点に関して、情報共有とそれを解決するための活動を行っている。今年度の活動は、DNSのセキュリティ脅威についての啓発のため、DNSへの攻撃を閉鎖環境で再現するエミュレータを作成した。また、WIDE研究会において本ワーキンググループのミーティングを定期的に開催し、DNSに関するホットトピックについて情報交換を行った。本報告書では、これらのミーティングにおいて発表、議論がなされた事項についてまとめる。

第２章　DNSへの攻撃エミュレータ

DNSは古くから存在するプロトコルであり、重要なインフラである一方いくつかのDNSに対する攻撃が判明している。その対策のためDNSSECが提案・実装されているが、特に日本において広く普及しているとは言い難い状態である。そこで、DNSSECの促進のため、詐称攻撃など、DNSに対する既知の攻撃を手軽に再現できるエミュレータの開発をおこなった。エミュレータはコンテナ環境上に構築され、コンテナオーケストレータとしてcontainerlabを利用する。エミュレータはコンテナ内のみで完結する形となっており、DNSツリーをルートネームサーバから構築し、それぞれのASをBGPルータで相互接続することで、現実のインフラを仮想的に再現している。攻撃手法は主にBGPハイジャックを悪用したDNSキャッシュ汚染攻撃であり、複数の攻撃シナリオを再現し、攻撃および被害時に発生する内容についてエミュレータ利用者が確認することができる。再現している攻撃シナリオは下記のとおりである。

1. Aレコードのキャッシュポイズニング
2. セカンダリへのゾーン転送の詐称
3. ACME validatorの詐称による電子証明書不正取得
4. パブリックDNSサーバのキャッシュ汚染
5. MXレコードの詐称によるメールの詐取
6. SPF/DKIM/DMARCレコードの詐称による不正メール送信

本エミュレータはさまざまなセキュリティ授業で利用することを想定し、広く配布を行う予定である。

第３章　WIDE合宿・研究会での議論まとめ

2024年は3月WIDE合宿、9月WIDE合宿、12月研究会にてDNS BOFが開催された。本節ではそれらのWIDE研究会におけるBOFでの議論についてまとめる。

3.1　惑星間インターネットでのDNSの課題と提案

Space WGのメンバーより、惑星間インターネットにおけるDNSのあり方について、議論提起があった。惑星間インターネットは既存の常時接続の地上インターネットと異なり、間欠的な接続性かつ秒～分単位の伝送遅延が存在する。そのため、従来の常時接続およびミリ秒レベルの伝送遅延を前提としているプロトコルをそのままで動作させることは困難である。そのため、Bundle Protocol（BP）など、耐遅延（Delay Torrelant）のプロトコルが考案されている。惑星間の通信はBPを用いて、惑星内の通信を既存のTCP/IPを用いるアーキテクチャを考えた場合、それぞれの惑星内および惑星間でDNSをどのように運用するかは大きな課題となる。惑星間をTLDで分割する、独自のルートを持ちそれぞれのネームスペースを完全に分離する、惑星ごとに代理のルートネームサーバを持ち別

惑星の名前については上書きする、などのいくつかの提案について紹介があった。議論では、それぞれのモデルについて名前解決時の問題、DNSSECで署名する際の問題、およびネームスペースを分けることでの相互接続性の問題などの課題が提起された。

3.2 DNSにおけるCNAMEチェーンの実態調査と改善のための標準化提案

JPRSの藤原氏より、CNAMEのチェーンが多段になっていることの問題と実態調査、およびその改善を含む提出中のインターネットドラフトについて紹介があった。現在、特にCDNに関する要求からCNAMEレコードが多段になっている例が多く見られている。調査結果から、3段以上のCNAMEチェーンを持つドメインは全体の中では少数であった。しかしながら、これらのドメインは主にCDNなどで利用されるドメイン名であるため、問い合わせ件数の割合は全体の10%以上を占めることが確認された。また、多段のCNAMEチェーンが名前解決のパフォーマンスに悪影響を出す実験結果について紹介があった。

現在のDNS関連のRFCではCNAMEチェーンの段数の制限について明示的に定められていないため、CNAMEチェーンの段数を含めたさまざまなDNSの動作上の上限を定める提案について、インターネットドラフト（draft-fujiwara-dnsop-dnsupper-limit-values-01）[94]が提出されており、そちらの内容についての紹介および議論が行われた。

第4章　まとめ

2024年のDNS WGでは、DNSのセキュリティ脅威に対する啓発を目的とした攻撃エミュレータの開発に取り組んだ。このエミュレータは、既知のDNS攻撃を閉鎖環境で再現可能にし、教育現場や研究において有用なツールとして活用されることを目指している。また、WIDE研究会における定期的なミーティングや議論を通じて、DNSに関連するさまざまなホットトピックを取り上げ、知見の共有と議論をおこなった。議論の中では、惑星間インターネットにおけるDNS運用の課題や、CNAMEチェーンの実態調査に基づく標準化提案について活発な議論をおこない、それぞれの分野での課題の共有をおこなった。DNSに関するホットトピックの情報共有および議論もWIDE合宿・研究会で継続的におこなっていく。