DNS暗号化がローカル / インターネットポリシーに与える影響

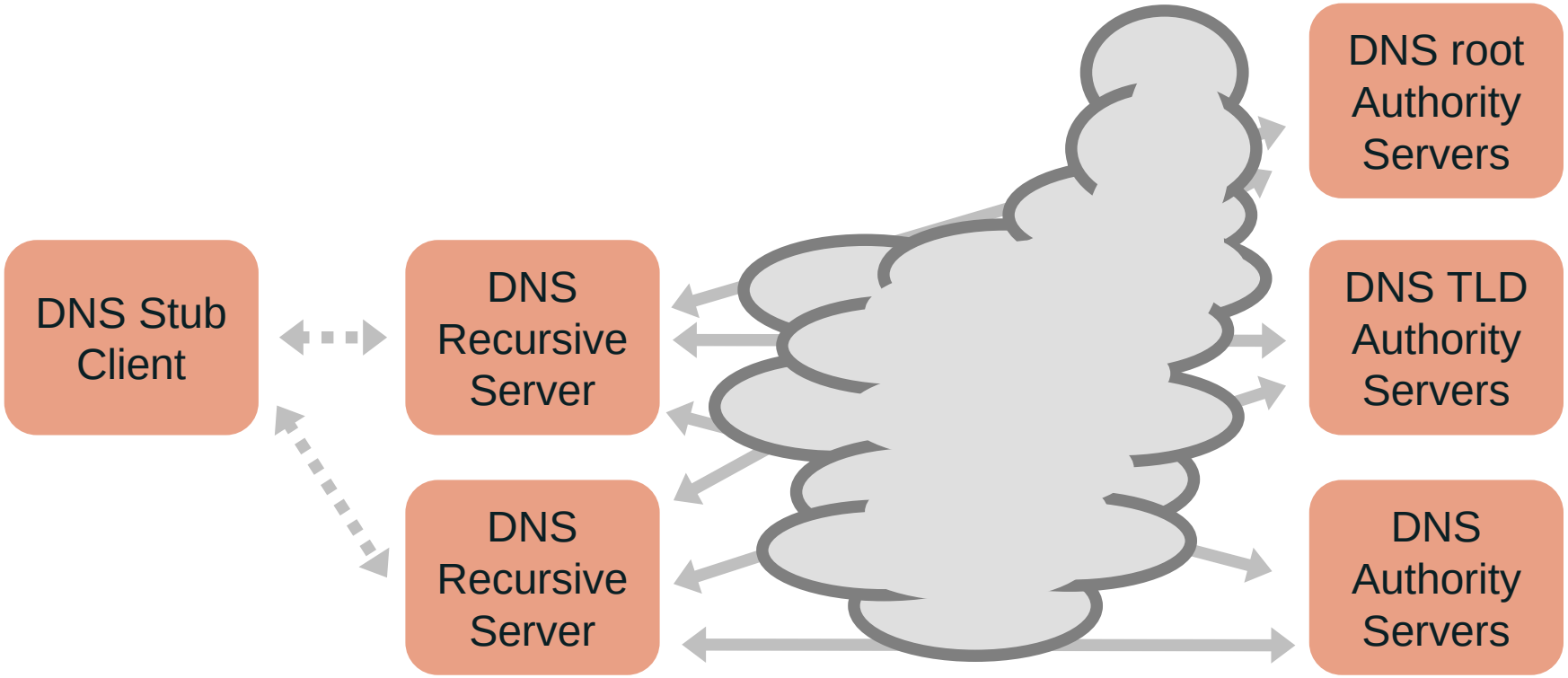
Paul Hoffman

ISOC-JPセミナー
2020年10月30日

ICANN's document (ICANNの文書)

- *Local and Internet Policy Implications of Encrypted DNS*
- https://www.icann.org/octo-003-en.pdf
- 第1版公開後、数回アップデート
- 主な話題：
  - DNSにおけるフィルタリングと監視
  - ポリシー面での影響
  - 利害関係者
  - ICANNの立場

DNS participants (DNSのクライアントとサーバー)



グレーの矢印は全て暗号化されていない通信

現在、「暗号化DNS」は上図左側の点線（DNSスタブクライアントからリカーシブサーバーへの線）を指す

DNS encryption: where (DNS暗号化：どこで)

- 今のところ、DNS暗号化はスタブリゾルバーで始まり、リカーシブリゾルバーで終わっている
- 最近まで、スタブリゾルバーはOSでのみ見られた
  - 全てのアプリケーションはDNSサービスのためにOSを呼び出す
- ここ数年で、ブラウザ（およびその他のブラウザに似たアプリケーション）が自らのスタブリゾルバーを追加するようになってきた
- DNS暗号化の標準では、クライアントがスタブリゾルバーの機能を、サーバーがリカーシブリゾルバーの機能を果たしていると想定

DNS encryption: how (DNS暗号化：その方法)

- 2つの標準プロトコル：
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)
  - 他に標準化されていないプロトコルもあるが、それらはあまり展開されていない
- DoT: https://datatracker.ietf.org/doc/rfc7858/
- DoH: https://datatracker.ietf.org/doc/rfc8484/
- DoTとDoHの間には重なる部分が多くあるが、ネットワークオペレーターにとっては違いが重要

DNS-over-TLS

- 基本的な仕組み：スタブリゾルバーがリゾルバーとTLSセッションを開始。セッションが確立されると、そこで通常のDNSトラフィックを送り始める
- リゾルバーの認証はオプションだが、中間者攻撃の防止に必要
  - 認証なしでも、外から監視している攻撃者にはトラフィックが読めない
- セットアップが簡単：必要なのはリゾルバーのIPアドレスまたはドメイン名のみ（ポート番号は固定）

DNS-over-HTTPS

- 基本的な仕組み：スタブリゾルバーがリゾルバーとHTTPSセッションを開始（通常のWebブラウジングと同様）。セッションが確立されると、そこでHTTPクエリに格納されたDNSトラフィックを送り始める
- HTTPのバージョンが2である場合、サーバーはクライアントにDNSコンテンツもプッシュすることができる。クライアントはそれを利用または破棄できる
- HTTPSで必須となっているため、リゾルバーの認証は必須
- セットアップはDoTより少し難しい：URLが必要
- DoHでは、サービスがURLに基づいているため、既存のHTTPS接続を再利用できる

Policy implications (ポリシー面での影響)

- ユーザーのDNSトラフィックでプライバシーが向上
- ユーザーのDNSトラフィックで確かさが向上
- セキュリティのためのDNSフィルタリングを迂回
- ローカルポリシーのためのDNSフィルタリングを迂回
- 政府に義務付けられたDNSフィルタリングを迂回
- DNS名前解決の望ましくない集中化を検知できない
- DNS応答の速度

Increased privacy and assurance (プライバシーと確かさの向上)

- 一般的にプライバシーは良いこと
- DNSトラフィックの暗号化により、スタブとリゾルバーの間にいる監視者からユーザーを守ることができる
- 暗号化により、攻撃者が応答のトラフィックを変更できないようにすることができる
- HTTPSをWebで使うのと同様、 DoTとDoHを使うことでDNSのセキュリティが向上する

Circumvention of filtering (フィルタリングの迂回)

- ネットワークオペレーターは、ユーザーのために、または少なくとも自社のシステムの健全性を維持するために、DNSを頻繁にフィルタリングまたは監視する
- セキュリティ（例：マルウェアの阻止）および/またはローカルポリシー（例：ペアレンタル・コントロール）のためにDNSをフィルタリングするミドルボックスは、DNS暗号化によって妨害される
- 特定の国/地域では、政府によって一部のフィルタリングが強制されている。そのため、フィルタリングを義務付けられた組織がDNS暗号化によって法令順守できなくなる可能性がある

Unwanted centralization (望ましくない集中化)

- DNS暗号化を実装しているクライアントは、DNS名前解決のためにOSまたはアプリケーションがどこへ行くかを変更できる
  - 暗号化されていないDNSでもできるが、そうすると変更されたことがより明らかになる
- これまでのところ、実施したことがあるのはFirefoxのみ
  - Firefoxは、利用者のデータをプライベートに維持するために特定のリゾルバーオペレーターだけを信頼している
  - 信頼できるプロバイダーのリストを持っているが、そのリストに載っているのは現在2社のみ
- プライバシー、多様性の低下によるレジリエンシーの低下や固定化などへの懸念

Speed of responses (応答のスピード)

- TLSセッションの開始は、ただ裸のDNSクエリを送るより本質的に遅い
- 過負荷のリゾルバーでは、TLSスタートアップの時間が長くなる可能性がある
- DoHでは、DNSクエリをHTTPメッセージに変更する必要もある
- しかし、初期のデータによれば、応答の90%はごくわずかに遅かったものの、10%ははるかに速かった。これは、TCPの信頼性がUDPより高いことによる

ICANN positions (ICANNの立場)

- プライバシーは良いこと
- DNSのフィルタリングは有益かもしれない
- アプリケーションとOSが持つ情報は、ネットワーク制御に関する決定をしたり、法律上の義務を履行したりするには不十分
- DNSデータは保護されるべき

Recent status (最近の状況)

- Mozillaは、信頼できる集中化された少数のリゾルバーを使い、世界のいろいろな地域でDoHを展開している
- Google Chromeでは、リゾルバーがDoTをサポートしている場合はDoTへ自動アップグレードする
- Microsoftは、DoH（DoTではなく）を使ったWindowsのリゾルバー接続のため安全なアップグレードを追加すると発表
- DNS暗号化の展開方法についての議論に参加するネットワークオペレーターが増えている