[ポスター発表] 研究報告

DNSにおける端末・権威サーバ間でのTLS通信による安全な名前解決

島袋 健大[1,a)]　阿久津 賢宏[1]　山井 成良[1,b)]　金 勇[2]　中川 令[1]

Secure Domain Name Resolution by Using TLS Communication between Stub Resolver and Authoritative DNS Servers

1. はじめに

今日においてインターネットは現代社会の根幹をなす重要な役割を果たしている. インターネットを実現している技術の一つとして, DNS と呼ばれる技術が存在するが, これはドメインと IP アドレスを結びつける役割がある. そして, クライアントから受け取ったドメインに対応する IP アドレスを返却する作業を名前解決と呼ばれているが, この名前解決は第三者からも確認することでき, 場合によっては通信内容を傍受されたり改竄されてしまう可能性がある.

このような攻撃に対する対策方法として, 名前解決によって得られたリソースレコードに電子署名を追加して内容が書き換えられていないか確認することができる DNSSEC と呼ばれる手法や, 名前解決で使われる通信路を暗号化することにより, 通信路の一部の区間でレコードの改竄と傍受を防ぐことができる DNS over TLS と呼ばれる手法が存在する. しかしながら, どちらの対策も完全には攻撃を防ぎきれない問題点がある.

本研究では名前解決で用いる通信路を暗号化することで通信傍受を防ぎ, 更にクライアント側で電子署名の検証を講じることで, なりすましを防ぐ.

2. 名前解決の問題点と既存の解決策の課題

前章で述べた通り, DNS による名前解決は平文で通信されることがある. その際に第三者によって通信内容を傍受される可能性があり, 結果知らないうちにクライアントがトラッキングされてしまう. また, 傍受してから通信内容の改竄も可能であり, フィッシング詐欺やマルウェア感染等の被害に遭ってしまう.

[1] 東京農工大学
Tokyo University of Agriculture and Technology.
[2] 東京工業大学
Tokyo Institute of Technology.
[a)] smb96@net.cs.tuat.ac.jp
[b)] nyamai@cc.tuat.ac.jp

このような攻撃の対策方法として DNSSEC や DNS over TLS と呼ばれる手法が存在するが, この手法にも問題がありそれは以下の通りである.

- DNSSEC(Domain Name System Security Extensions) の場合
  DNSSEC[1] とは, 名前解決を行う際に権威サーバからレコードと正当な権威サーバであることを示す電子署名を送る手法であり, これにより第三者によってレコードを改竄された場合に, これをクライアントで検知が可能になる.[2] 但し, レコードの傍受を防ぐことはできず, 名前解決を行うドメインの深さ次第では処理に時間がかかってしまう問題が挙げられる.
- DoT(DNS over TLS) の場合
  DoT[3] とは, クライアントからキャッシュサーバにクエリを送信する際に暗号化通信を行い, キャッシュサーバから権威サーバは平文で通信する手法であり, これによりクライアントとキャッシュサーバ間では第三者による介入が存在しない安全な通信が実現できる. 但し, キャッシュサーバと権威サーバ間では依然攻撃を受けるリスクがあり, 更に権威サーバ自体が攻撃されて偽のレコードが仕組まれている場合は, これを検知することができない問題 [4] が挙げられる.

3. 安全な DNS 名前解決手法の提案

本研究では名前解決の際にクライアントがキャッシュサーバから権威サーバのアドレスを取得し, その後 DNS over TLS を用いてクライアントが直接権威サーバに暗号化通信を行うことで, 安全な名前解決が実現できることを提案する. 更に, 権威サーバを設置している組織の殆どが OV 証明書や EV 証明書を導入していることを利用し, クライアントが権威サーバの SSL 証明書を参照し, 証明書の内容から権威サーバが信頼できるか否かを判定することで, 名前解決中の安全性をより高める仕組みを作成する. 提案する名前解決の手法を図 1 に示す.

但し, 今回正規の権威サーバに対して不正アクセスされて偽のリソースレコードが混入されることはなく, クライアント側は権威サーバの IP アドレスが既知である前提である. また, この手法を行う場合, キャッシュを用いないことから権威サーバへの負担が懸念されるが, キャッシュを用いない名前解決は DNS round robin でも利用されていたり, 名前解決自体負荷のかからない処理であるため, 問題にならないと考えられる.

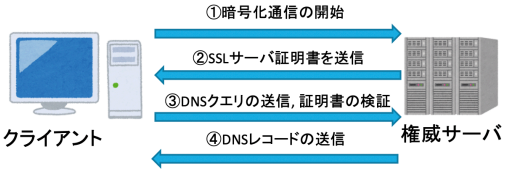

図 1 提案する名前解決の手法

4. 安全な DNS 名前解決手法の実装

提案した手法を実装するために, Python の dnslib ライブラリを用いて本手法を実装し, 動作検証を行った. 次に, 実装したシステムの動作手順と検証結果を解説する.

4.1 提案手法の動作手順

(1) 権威サーバが TLS 通信用のソケットを確保し, クライアントからの接続を待機する.
(2) 同様にクライアント側も TLS 通信用のソケットを確保し, 権威サーバへ接続を試みる.
(3) 権威サーバが接続を許可して暗号化が開始し, その際にサーバの保有している SSL 証明書をクライアントに送信する.
(4) クライアントが権威サーバに名前解決の要求クエリを送信すると同時に, 権威サーバから入手した証明書の内容をフィールドの個数を元にチェックする.
(5) 証明書が DV 証明書である場合, 権威サーバが信頼できないものであるとし, ターミナル上に警告のメッセージを出力する.
(6) 証明書が OV, EV 証明書である場合, 権威サーバが信頼できるものとし, そのまま名前解決を続行する.
(7) 権威サーバが名前解決した結果をクライアントに送信する. クライアント側は結果を表示し通信ソケットを切断する.

4.2 提案手法の動作結果

実装したシステムを用いて, 実際に暗号化通信と SSL 証明書による権威サーバの推定ができているか検証を行った. 検証方法として, 権威サーバに DV 証明書, OV 証明書を導入した状態でクライアントからの名前解決を行い, 安全であるか判断を行った.

検証の結果, OV 証明書の場合はドメイン以外のフィールドも記入されていることを確認し, 信頼できるものとして判定された. 一方, DV 証明書の場合はドメインフィールドしか記載されていないため, 権威サーバを信頼できず改めて権威サーバの情報を確認するよう警告メッセージが出された.

```
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22393
;; flags: rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;google.com.                    IN      A

;; Certification Information:
;; countryName: JP
;; stateOrProvinceName: Tokyo
;; localityName: Shinjuku
;; organizationName: Y-lab
;; organizationalUnitName: in 209
;; commonName: OV_Cert

Subject domain is using OV or EV certfication.
```

図 2 OV 証明書を用いた権威サーバに対する名前解決の結果

```
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61762
;; flags: rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;google.com.                    IN      A

;; Certification Information:
;; commonName: DV_cert

WARNING! Subject domain is using DV certfication. Recommend you checking site.
```

図 3 DV 証明書を用いた権威サーバに対する名前解決の結果

5. おわりに

本研究では, DNS の名前解決時に全通信区間で安全に処理する手法と, 通信する際の権威サーバの正当性を SSL 証明書を用いて判別する手法を提案した.

今後の課題としては, クライアントが権威サーバの IP アドレスを保有する手法や, 権威サーバのより詳しい正当性検証といった実際に運用する上で想定される課題を解消する必要がある. また, 本手法では DoT を基盤にしたが, DoT に似た別の名前解決の手法との性能比較をするべきであると考えられる.

参考文献

[1] ”RFC 4033 - DNS Security Introduction and Requirements”, https://tools.ietf.org/html/rfc4033, Accessed: 2021-10-24.
[2] ”インターネット 10 分講座：DNSSEC - JPNIC”, https://www.nic.ad.jp/ja/newsletter/No43/0800.html, Accessed: 2021-10-24.
[3] ”RFC 7858 - Specification for DNS over Transport Layer Security (TLS)”, https://tools.ietf.org/html/rfc7626, Accessed: 2021-10-24.
[4] ”インターネット 10 分講座：DNS キャッシュポイズニング - JPNIC”, https://www.nic.ad.jp/ja/newsletter/No40/0800.html, 2021-10-24.