N-014

# 情報セキュリティ教育のための DNS サービス/DNS キャッシュポイズニング可視化システム －キャッシュポイズニング可視化機能の改善－

# Visualization System of DNS service and DNS Cache Poisoning Attack for Information Security Education － Improved Visualization of Cache Poisoning －

後藤 祥仁† 米谷 雄介† 喜田 弘司† 最所 圭三†
Yoshihito Goto　Yusuke Kometani　Koji Kida　Keizo Saisho

## 1. はじめに

DNS サービスは，インターネットにおいて根幹のシステムであり，ドメイン名と IP アドレスの対応関係を管理する．そのため，サイバー攻撃の対象とされることも多く，中でも DNS キャッシュポイズニングが代表的な攻撃として挙げられる．すでに防御策は公知であるが，完全ではないため，DNS への攻撃は後を絶たない[1]．そこで，DNS キャッシュポイズニングを理解しておくことは情報系学生にとって重要である．しかし，多くの大学では概念的な説明にとどまっている．そのため，実際に目に見えないものを，DNS を初めて習った初学者がいきなり理解することは難しい．そこで我々は，多数の初学者が DNS サービスと DNS キャッシュポイズニングを視覚的に確認できる可視化システム「Visual DNS Attack(VDA)」を開発してきた[2].

本稿では，先行研究で開発した VDA(VDA.v1)の評価結果に基づいて，改善した VDA(VDA.v2)について述べる．

## 2. VDA の概要

初学者が，DNS サービスおよび DNS キャッシュポイズニングを自学自習できることを目的に VDA を開発している．図 1 に VDA の UI を示す．初学者が各自使用するため，実行環境を選ばない Web アプリケーションで実装を行う．

VDA は以下の 3 つの機能を有している．

機能①：パケットの流れをその目的が埋め込まれた矢印で順に描画する．これにより，DNS における問い合わせの手順を学習できる．

機能②：DNS キャッシュの有無によるパケットの流れを変える．これにより，キャッシュサーバにユーザからドメイン名に対する問い合わせが来たとき，キャッシュに該当のドメイン名があればその IP アドレスを返し，ないときはドメイン情報を権威サーバにアクセスすることを学習できる．

機能③：ユーザサイドとクラッカーサイドを分割する．これにより，偽 IP アドレスを DNS キャッシュに仕掛けるクラッカーサイドと，DNS キャッシュに仕掛けられた偽 IP アドレスにアクセスしてしまうユーザサイド，それぞれの立ち位置で学習できる．

これらの機能により，ドメイン名から IP アドレスを取得するまでのやり取りを順番に追いかけることができる．さらに，キャッシュポイズニングによって偽 IP アドレスがキャッシュサーバに方法と，その偽 IP アドレスに対してユーザがアクセスしてしまう方法を，通信の流れを見ながら確認することができる．

†香川大学　Kagawa University


図 1　VDA の UI

## 3. VDA.v1 の評価および改善策

VDA.v1 を用いることによる教育効果について述べる．

DNS の動作とキャッシュポイズニングにより偽 IP アドレスへ誘導されることが，理解しやすくなるのかを確認するための評価を行なった．VDA.v1 を使って学習した香川大学創造工学部学部生に，DNS サービス及び DNS キャッシュポイズニングの理解度についてアンケートを実施した．その結果，6 種類の質問に対して DNS の動作や攻撃されることによる弊害について 7~8 割の学生が「理解できた」と回答した．しかし，キャッシュポイズニング攻撃が失敗する原因の理解度に比べ，成功する原因の理解度が 1 割ほど少なかった．

VDA.v1 では，本来の IP アドレスではなく，クラッカーが用意した偽 IP アドレスを得てしまうことに注力した．その結果，キャッシュがないだけでポイズニングが成功するようにしていた．キャッシュポイズニング手法の可視化をより現実に近づけることで，初学者がキャッシュポイズニング手法の理解が深まり，同時に DNS サービスの構造やその欠点についての理解も深まると考えた．

VDA.v1 では，キャッシュサーバが権威サーバから応答パケットを受け取るときに，本来行われるトランザクション ID(TxID)のチェックをしていなかった．そこで，問い合わせ時に指定した TxID と，応答パケットに含まれる TxID が一致したとき，正規のパケットとして受理されることを可視化した．クラッカーはこの TxID が一致するまでキャッシュサーバにパケットを送信し続け，TxID が一致した時，ポイズニングが成功したことになる．そこで，キャッシュする条件に TxID の検査を加えることにした．これにより，TxID により応答パケットが正しいかどうか判断し

ていること，TxID が一致する偽 IP アドレスのパケットが送り込まれてキャッシュポイズニングに成功すること，の 2 つを理解させることができると考えた．

これらの検討により，以下の 2 つの改善方法を提案する．

改善①：TxID による応答パケットの正誤判定を行う．VDA.v1 では，キャッシュサーバが無条件でパケットを受け入れる形になっていたが，この改善によって TxID が一致すれば応答パケットを受け入れることがわかる．

改善②：クラッカーがキャッシュポイズニングに成功するまで攻撃を繰り返す．攻撃回数の上限を指定できる．VDA.v1 では，キャッシュの有無のみで攻撃の可否を判定していたが，この改善によって TxID によって防御できることがわかる．

次節では，これらを組み込んだ VDA.v2 について述べる．

## 4. VDA.v2 における可視化システム機能の改善

### 4.1 TxID を用いた正誤判定

送信した TxID と，受信したパケットの TxID が一致したときにパケットを受け入れることを可視化した．図 2 に権威サーバからの応答のようすを示す．キャッシュサーバの下に，権威サーバへの問い合わせ時に自動的に生成された TxID(b)を表示する．さらに，権威サーバへの問い合わせ時や，権威サーバからの応答が来る際，パケットの説明と同時に TxID(a)も表示する．これにより，TxID によってその通信が正しいかどうかを判定していることが理解できると考えた．

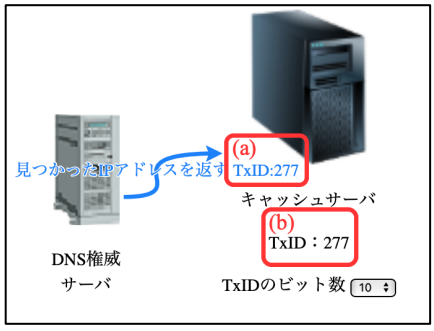


図 2　TxID を追加した実装

### 4.2 クラッカーによるキャッシュサーバへの攻撃

クラッカーが権威サーバよりも先に一致する TxID を持つ応答パケットをキャッシュサーバに送ると，キャッシュポイズニングが成功することを可視化する．さらに，何度もキャッシュサーバにアクセスしていることがわかるようにする．また，クラッカーサイドに攻撃回数上限を選択できるようにし，偽 IP アドレスを送り込むことに失敗することも可視化する．TxID のビット数は本来 16 ビットであるが，2 ビットから 16 ビットまで変更できるようにする．これにより，ビット数により攻撃成功確率が変動することを理解できる．

図 3 に 1 回目攻撃時の可視化のようすを，図 4 にクラッカーサイドの攻撃回数の設定を示す．攻撃方法をわかりやすくするため，1 回目のみ図 3 のような形で実装している．2 回目以降の攻撃は，TxID を変えただけで他は変わらない．2 回目以降の攻撃であることを表現するため，矢印を複数並べて表示するようにした．

クラッカーの攻撃上限回数を図 4 に示すように設定できる．これにより，クラッカーの攻撃回数が足りないことによる，攻撃の失敗の様子を見せることができる．

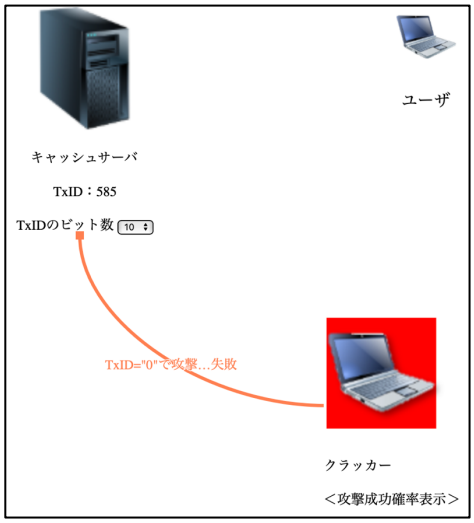


図 3　TxID=0 での最初の攻撃のようす


図 4　クラッカーサイドでの攻撃回数の設定

### 4.3 使用方法

キャッシュサーバが権威サーバに IP アドレスを問い合わせる際に TxID が表示される．そのため，まずはユーザサイドでキャッシュサーバにキャッシュされていないドメイン名を問い合わせる動作を行う．これにより，初学者は TxID が DNS サービスにおいてどのような働きをしているかを理解することができる，と考えている．

TxID のビット数の変更に伴い，攻撃成功確率もクラッカーサイドで攻撃を行うごとに表示される．そのため，初学者は TxID のビット数によって攻撃成功確率も変動することがわかる，と考えている．

## 5. おわりに

本論文では，TxID によるパケット正誤判定と，それによるクラッカーの攻撃可否による VDA の改善と実装を述べた．今後，ユーザによる評価を行う予定である．

### 参考文献

[1] Man K., Qjan Z., Wang Z., Zheng X., Huang Y., and Duan, “DNS Cache Poisoning Attack Reloaded: Revolutions with SideChannels”, Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp.1337-1350(2020)

[2] 後藤祥仁, 米谷雄介, 喜田弘司, 今井慈郎, 最所圭三, “情報セキュリティ教育における DNS サービスおよび DNS キャッシュポイズニングの可視化 -Web アプリの開発と評価- ”, 教育システム情報学会 2020 年度学生研究発表会 四国地区, No.221, 222 (2021).