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-

Visualization of DNS service and DNS Cache Poisoning Attack for Information Security Education
- Development and Evaluation of Web-based Application -

後藤 祥仁，米谷 雄介，喜田 弘司，今井慈郎，最所圭三
Yoshihito GOTO, Yusuke KOMETANI, Koji KIDA, Yoshiro IMAI, Keizo SAISHO
香川大学
Kagawa University
Email: s17t234@stu.kagawa-u.ac.jp

あらまし：我々は多数の学習者が DNS 機能を視覚的に確認できるシステム「Visual DNS Attack」を開発した．本システムの特徴として，LeaderLine を用いた通信の流れや，キャッシュサーバ内のデータを可視化，キャッシュポイズニングをハッカーが偽 IP アドレス挿入してユーザがそれに引っかかるという構図にする，などが挙げられる．5 段階評価で受講者に対してアンケート行った結果，6 割以上が理解できたと回答し，教育効果があったことが確認できた．
キーワード：教育支援システム，可視化，DNS，Web アプリケーション

1. はじめに

DNS は 1983 年頃に考えられた，ドメイン名と IP アドレスの対応関係を管理するインターネットの根幹のシステムである．しかし，黎明期に確立された仕組みであるため，オープンリゾルバなどの脆弱性が多い(1)．その中でも代表的な攻撃が DNS キャッシュポイズニングである．すでに防御策は出ているが，それを本にした攻撃手法は後を絶たない(2)．

そのため，DNS キャッシュポイズニングを理解しておくことは重要であると考える．しかし，多くの情報系の大学では概念的な説明にとどまっており，実物として存在しないものをイメージするのは，初学者にとって分かりにくい．

そこで，理解を促すためのシステムが必要であると考えた．我々は，通信の流れとその目的が視覚的にわかること(課題 1)，キャッシュサーバのデータによって IP アドレスの取得方法などが変わること(課題 2)，キャッシュポイズニングがキャッシュサーバのデータを書き換えるのではなく偽 IP アドレスを挿入していること(課題 3)，の 3 点が分かることを課題として定めた．

2. システム開発

2.1 システム概要

我々は先ほど挙げた課題を解決するため「Visual DNS Attack」を開発した．図 1 に Visual DNS Attack のユーザインターフェース(UI)を示す．本システムは，講義で先生が受講者に向けて実際に使用しながら説明，その後受講者が各々使用することで理解を深めさせる．受講者が各々使用するため，気軽に利用できる Web アプリケーションで実装を行う．

図 1 Visual DNS Attack の UI

2.2 課題解決方法

課題 1 を解決するため，LeaderLine(3)を用いた．これは引き出し線を描画するためのプログラミングライブラリであり，図 1 の可視化部分に表示されているように矢印を描画することができる．これにより通信の流れを可視化できる．ボタン群のボタンを押すことで DNS の名前解決やキャッシュポイズニングによる偽 IP アドレスの挿入の手順を矢印で表示される．また，矢印中に文字を埋め込むことができるため，その通信が何のために何をしているかがわかる．

課題 2 を解決するため，キャッシュサーバのデー

タを可視化した．キャッシュサーバのデータを可視化部分の下側に配置している．キャッシュサーバのデータに応じて矢印遷移も自動的に変化するようになっており，初学者がキャッシュサーバのデータを見ながら矢印遷移も確認できるようになっている．

課題 3 を解決するため，ボタン群でユーザサイドとハッカーサイドに分けた．ユーザサイドがキャッシュサーバから IP アドレスの取得, ハッカーサイドがキャッシュサーバに偽 IP アドレスの挿入を行う．このようにすることで, ハッカーサイドで偽 IP アドレスを挿入した後, ユーザサイドで偽 IP アドレスを取得してしまうという構図ができ，より現実に即した可視化になり理解しやすくなると考えた．

3. 利用者によるシステム評価

3.1 評価方法

Visual DNS Attack を実際に使用して講義を行うことで, DNS の動作や攻撃手法を理解しやすくなるのかどうかを確認する．そのため，本システムについて全く知らない第三者視点での評価を行う．

評価は Google フォームを用いたアンケート形式で表 1 の 5 段階評価の 7 項目と，自由記述の計 8 項目で行う．課題 1 は項目 1，2，課題 2 は項目 1，2，3，5，課題 3 は項目 4 の評価の高さで達成できたかを見る．6 は操作性, 7 は本システムの必要性を見るために設置した．アンケート対象者は香川大学創造工学部 1 年次配当授業「論理回路」の受講者である．講義はオンラインで，情報系は必修科目である．

3.2 評価結果

表 2 に表 1 の評価項目の評価結果を示している．アンケートを実施した結果, 回答数は 67 票であった．

表 1　5 段階評価の評価項目

No.	質問内容
1	キャッシュサーバ上に関連するドメイン名と IP アドレスがある時とない時で, IP アドレス取得までの流れが変わることが理解できたか
2	キャッシュサーバに上に関連するドメイン名と IP アドレスがない時，権威サーバから IP アドレスを取得する流れを理解できたか
3	キャッシュに攻撃目標のドメイン名がなかった時，キャッシュポイズニングを実行できることが理解できたか
4	ユーザ側からみるとドメイン名と紐づけられている IP アドレスが書き換えられたように見えるが，実際には偽情報がキャッシュサーバに送り込まれていることが理解できたか
5	キャッシュサーバに, 攻撃目標のドメイン名のキャッシュが残っていると攻撃できないことが理解できたか
6	DNS と DNS キャッシュポイズニングの仕組みを理解するうえで，Visual DNS Attack を容易に操作できたか
7	Visual DNS Attack によってどのように IP アドレスの書き換えが発生するのかを理解できたか

表 2 評価結果

No.	よく理解できた	だいたい理解できた	どちらともいえない	あまり理解できない	全く理解できない
1	41%	38%	15%	4%	1%
2	41%	35%	15%	9%	0%
3	38%	35%	15%	12%	0%
4	41%	34%	18%	7%	0%
5	37%	43%	16%	3%	1%
6	24%	44%	22%	10%	0%
7	31%	46%	18%	4%	1%

表 2 から，1~5，7 で「よく理解できた」「だいたい理解できた」と答えた割合が 7 割を超えており，6 が他と比べて低いことが分かる．また，自由記述では 10 件の回答を得ることができ，3 つが悪い点，6 つがよい点, 1 つがよい点悪い点両方書かれていた．

3.3 考察

全体的に高い評価を得ることができ，Visual DNS Attack は理解を促すうえで効果があったと考えられる. しかし, 項目 6 が他と比べると評価が低かった．項目 6 は操作性が難しすぎないかどうかを問うている．操作性が難しいと理解を促すのに弊害が出てしまうと考えていたため，他の項目よりは評価が高くなると予想していた．しかし，操作性が難しくとも理解を促すことができていた．これは 2.1 節で挙げた使用方法にあると考える．評価実験も同じ方法で使用しており，講義で先生が実際に使用しながら説明した段階で，多くの受講者が理解できていたということになる．つまり，講義で受講者に対して見せるだけでも十分効果があったと考えられる．

また，自由記述の悪い点の中に,「矢印の流れの速さがデフォルトだと早い」という意見があった．ボタン群には自動遷移と矢印一つずつステップ実行があり，自動遷移の速さが早いと書かれていた．デフォルトで速いと感じた受講生は他にもいると考えられるため，少し遅くする必要があると考えた．

4. おわりに

DNS と DNS キャッシュポイズニングを可視化する「Visual DNS Attack」を開発し，理解を促すうえで効果があったと考えられると結論付けた．

参考文献

(1) 勝村幸博: “「悪質サイト勝手にリダイレクト」---DNS キャッシュ・ポイズニング攻撃の現状と対策(上)” (https://xtech.nikkei.com/it/free/ITPro/OPINION/20050411/158828/)(参照 2021.2.8)

(2) 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)

(3) anseki: “LeaderLine”, https://anseki.github.io/leader-line/ (参照 2021.2.8)