氏　　名　GUANNAN HU

学位(専攻分野)　博士(情報学)

学 位 記 番 号　総研大甲第 2527 号

学位授与の日付　2024 年 9 月 27 日

学位授与の要件　複合科学研究科　情報学専攻
学位規則第6条第1項該当

学 位 論 文 題 目　Privacy Leakage in Encrypted DNS Traffic: Analysis and Countermeasure

論 文 審 査 委 員　主　査　福田　健介
情報学コース　教授
計　宇生
情報学コース　教授
金子　めぐみ
情報学コース　教授
鯉渕　道紘
情報学コース　教授
落合　秀也
東京大学　大学院情報理工学系研究科　准教授

Summary of Doctoral Thesis

Name in full GUANNAN HU

Title
Privacy Leakage in Encrypted DNS Traffic: Analysis and Countermeasure

The Domain Name System (DNS) translates domain names into one or more IP addresses by asking the caching server when the users enter a URL into their browser. The DNS caching resolver stores a database of domain names and their corresponding IP addresses in the global network. While the user types a domain name into the web browser, the host first checks the caching resolver to see if it already has the corresponding IP address. If no, it begins by querying a root server, then the top-level-domain (TLD) server, and finally the authoritative name server.
DNS is designed to be sent in plain text according to RFC 1035, allowing the adversary to eavesdrop on DNS communication by monitoring the network. DNS messages are unencrypted and contain domain names representing the users' private information, such as health, finance, and religion, which leads to information leakage while users visit websites. Intending to protect the person's private information, several encrypted DNS protocols have been proposed: DNS over HTTPS (DoH), DNS over TLS (DoT), and DNS over QUIC (DoQ). These protocols encrypt DNS packets between the client and DNS caching resolver with different underlying transports. Some public DNS caching resolvers have already supported DoT and DoH, such as Google, Cloudflare, and Quad9. Only the AdGuard and NextDNS support the DoQ protocol, at the time of writing. Also, the user could change the settings of some browsers (e.g., Chrome and Firefox) to enable the DoH. However, recent studies showed that the adversary could still infer the category of websites even using DoT and DoH by analyzing the encrypting DNS traffic. The goals of this dissertation are to investigate the information leakage problem of encrypted DNS protocols and develop countermeasures to protect user privacy against website fingerprinting attacks.
In the first half of this dissertation, we study the privacy leakage problem of encrypted DNS traffic (i.e., DoT, DoH, and DoQ) with three different DNS caching resolvers (NextDNS, Bind, and Google). Depending on the DNS software configurations (public and local DNS caching resolvers), we consider two threat models to simulate the website fingerprinting on binary and multi-classification. We choose 30 categories from Alexa's top 300,000

websites and select the top-400 websites for each category. For the binary classification, we split the dataset into 'Sensitive', related to personal information such as health, finances, religion, and government, and 'Non-Sensitive'. As the baseline analysis, we evaluate the classification performance of DoQ traffic with balanced (10 categories from 'Sensitive', and 10 categories from 'Non-Sensitive' randomly) and imbalanced (10 categories from 'Sensitive', and remaining 20 categories from 'Non-Sensitive') datasets on Bind and NextDNS. We also examine the performance of DoQ, DoH, and DoT with Google resolver. We find that the classification performance of the websites is high both in NextDNS, Bind, and Google resolvers for identifying whether the user visits the category of websites. We confirm no significant influence on whether the local resolver is cached and caching order. More particularly, we indicate that discriminative features are mainly related to the inter-arrival time of packets and packet length. For the multi-classification, we notice the performances decrease as the number of categories increases for the Bind resolver, meaning that the impact of the leakage is limited. We also notice the performances are not directly related to the number of crawls.

From the important features, a promising approach is to control the inter-arrival distribution and packet length for the mitigation. In the second half of this dissertation, we further investigate four possible countermeasures that could affect the classification results: using AdBlocker extension, disabling DNS prefetch, adding random delay in responses, and padding the DNS payload. 1) We show that using AdBlocker and disabling DNS prefetch are less effective in mitigating the attack. 2) We find that mean F1 scores decrease as the delays increase. Specifically, it decreases the classification performance by 22% with NextDNS and 18% with Bind. 3) DNS padding decreases the classification performance by 9%. We further investigate the combination of the two countermeasures: both adding random (0-60ms and 0-100ms) delays and padding the DNS payload. We confirm that the combined method could greatly reduce the classification performance, on average 27% of binary and 22% of multi-classification in Bind. These results indicate that adding random time and padding can protect users' information from the website fingerprinting attack.

（別紙 Separate Sheet）

Results of the Doctoral Thesis Defense

博士論文審査結果

Name in Full
氏　　名　GUANNAN HU

Ｔｉｔｌｅ
論文題目　Privacy Leakage in Encrypted DNS Traffic: Analysis and Countermeasure

本学位論文は、「Privacy Leakage in Encrypted DNS Traffic: Analysis and Countermeasure」と題し、英文で記述され、全七章から構成されている。

第一章「Introduction」では、悪意のあるユーザによるウェブブラウジングにおけるプライバシ情報漏洩における研究分野の概況と本研究の目的を述べている。本章ではウェブブラウジングをターゲットとしたWFP（Website Fingerprinting）攻撃について述べ、既存の暗号化されたウェブトラフィックやDNSトラフィックにおけるプライバシに漏洩の問題を指摘している。そして、本論文の目的が、これらの問題の影響を測定によって明らかにし、その対応策について評価を行うことであると述べている。

第二章「Background and Related Works」では、暗号化DNS通信プロトコルの概説と現在の導入状況、ウェブトラフィックにおけるWFP攻撃およびDNSトラフィックにおけるWFP攻撃に関する研究動向をまとめている。

第三章「Methodology」では、暗号化DNSトラフィックにおけるWFP攻撃の実験方法について述べている。ネットワーク環境、利用DNSプロトコル実装、対象ウェブサイトの分類、トラフィック特徴量抽出、機械学習アルゴリズムの検討等について説明がされている。

第四章「Classification Performance」では、暗号化DNSトラフィックにおけるWFP攻撃によってどの程度の精度で閲覧ウェブサイトのカテゴリ(二値、多値)が推定可能かを調査している。実験結果より、利用DNSプロトコルおよびその複数実装、ローカル・パブリックDNSの違いに関わらず、二値分類（sensitive, non-sensitive）では十分高い性能で分類が可能であり、多値分類では現実的には分類が難しいことを定量的に示している。また、分類に関して特徴量の影響を調査し、DNSクエリ・応答の到着時間間隔分布およびDNSクエリ・応答のパケット長が分類性能に大きく影響を与えていることを明らかにした。

第五章「Countermeasure」では、上記の特徴量をプロトコル・実装レベルで制御することで、分類性能を下げることが可能であるかについて、複数の対策手法を調査している。実験結果より、AdblockerやDNSプリフェッチでは余り効果が見られないものの、クエリ間でランダムな遅延を挟むこと、クエリ・応答パケット長をパディングすることで、その分類性能を 27%程度緩和できることが示された。

第六章「Discussion」では、評価のまとめ、ステークホルダーへの提言、実験手法の限界、今後の課題について述べ、第七章「Conclusion」では結論を述べている。

公開発表会では博士論文の章立てに従って発表が行われ、その後に行われた論文審査会及び口述試験では、審査員からの質疑に対して適切に回答がなされた。質疑応答後に審査委員会を開催し、審

査員で議論を行った。審査委員会では、出願者の博士研究がユーザのウェブブラウジング時のプライバシ向上に貢献することが評価された。

以上要するに本学位論文は、ユーザのウェブブラウジング時に問題となりうる暗号化 DNS トラフィックの WFP 攻撃の可能性について定量的に評価し、その対応策の検討及びその有用性を示したものである。また、本学位論文の成果は、学術雑誌論文一件、フルペーパー査読付国際会議論文一件として発表され、学術的な貢献も認められる。以上の理由により、審査委員会は、本学位論文が学位の授与に値すると判断した。