# Privacy-Risiken durch DNS

## Extrahierung personenbezogener Daten aus DNS-Abfragen und Wirksamkeit von Schutzmechanismen


Studenten

**Baruyr Bousnaian**

**Ivo Andri Cavelti**


Ausgangslage: Das Domain Name System (DNS) ist eine zentrale Komponente der Internet-Infrastruktur und wird bei allen gängigen Online-Aktivitäten verwendet. In seiner ursprünglichen Form wurde DNS jedoch ohne Fokus auf Datenschutz entworfen. Abfragen werden standardmässig unverschlüsselt übertragen und erlauben beteiligten Akteuren Rückschlüsse auf das Nutzungsverhalten einzelner Personen zu ziehen.

Zur Reduktion dieser Risiken wurden Obfuscation-Mechanismen wie DNS over HTTPS (DoH) entwickelt, welche den Inhalt der DNS-Anfragen verschlüsseln. Dennoch zeigen Studien, dass bei verschlüsseltem DNS weiterhin Metadaten für Fingerprinting sichtbar bleiben.

Diese Arbeit untersucht, welche Informationen aus DNS-Traffic extrahiert werden können und wie effektiv moderne Schutzmechanismen diese Informationsgewinnung einschränken.

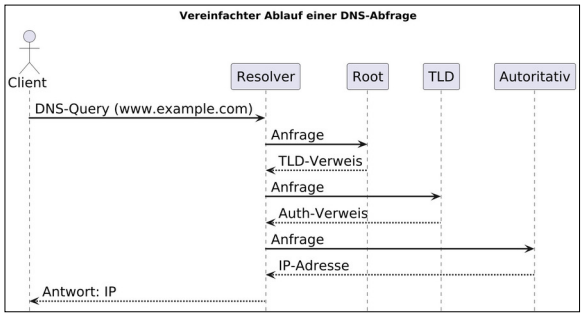
Vorgehen: Ziel der Arbeit ist die systematische Analyse von Privacy-Risiken im DNS-Traffic und die Bewertung moderner Schutzmechanismen. Dazu wurde eine modulare, reproduzierbare Analysepipeline in Python entwickelt, welche DNS-Traffic aus PCAP-Dateien verarbeitet und daraus Merkmale extrahiert.

Als Datengrundlage wurden synthetisch erzeugte Szenarien sowie öffentliche Datensätze verwendet und unter unterschiedlichen DNS-Konfigurationen aufgezeichnet. Neben der Analyse von unverschlüsseltem DNS lag ein besonderer Fokus auf DoH. In einem Experiment wurde der verbleibende Metadaten-Leakage bei DoH untersucht, indem wiederholt automatisierte Webseitenaufrufe ausgeführt und ausschliesslich der DoH-Traffic ausgewertet. Anhand aggregierter Merkmale wie Paketanzahl, Datenvolumen und zeitlicher Struktur wurde analysiert, ob sich unterschiedliche Aktivitätsklassen trotz verschlüsselter DNS-Inhalte unterscheiden lassen.

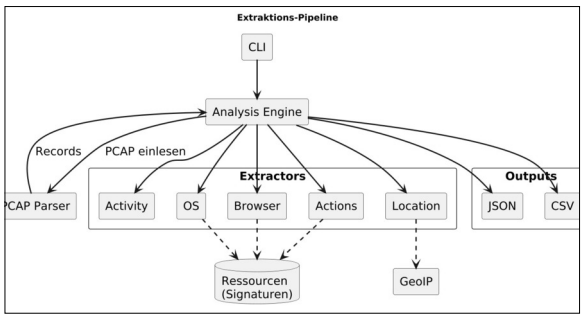
Fazit: Die Ergebnisse zeigen, dass sich aus unverschlüsselten DNS-Abfragen umfangreiche personen- und verhaltensbezogene Informationen ableiten lassen. Schutzmechanismen wie dass DNS over HTTPS (DoH) reduzieren diese Informationspreisgabe erheblich, da der direkte Zugriff auf Domainnamen und weitere DNS-Inhalte entfällt.

Gleichzeitig zeigt unser Experiment, dass DoH keinen vollständigen Schutz bietet. Metadaten wie Anfragefrequenzen, Datenvolumen und zeitliche Muster bleiben sichtbar und erlauben weiterhin Rückschlüsse auf Nutzeraktivitäten.
Insgesamt bestätigt die Arbeit, dass verschlüsseltes DNS einen wichtigen Beitrag zum Datenschutz leistet, jedoch keine vollständige Eliminierung von Privacy-Risiken erreicht. Obfuscation-Massnahmen sind zu empfehlen, sollten jedoch im Kontext eines realistischen Threat-Models betrachtet werden.

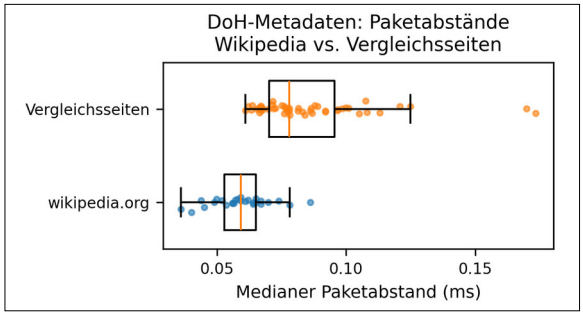
**DNS-Abfrage: Client fragt Resolver, der über Root/TLD den autoritativen Server findet und die IP liefert.**
Eigene Darstellung




**Analysepipeline: CLI steuert Engine, Parser liefert Records, Extractors erzeugen Merkmale, Export als JSON/CSV.**
Eigene Darstellung




**Medianer DoH Paketabstand: Wikipedia vs. Vergleichsseiten. Metadaten erlauben Rückschlüsse auf Aktivität.**
Eigene Darstellung




Referent
**Prof. Dr. Daniel Patrick Politze**

Themengebiet
**Internet-Technologien und -Anwendungen, Data Science, Software**