# DNS TUNNELING ISSUES

Jack Lin

Computer Networks - COSC 4378

Computer Science/Electrical Engineering

## Section I: Abstract

- Introduction to DNS as an Internet cornerstone.
- Explanation of DNS vulnerabilities and DNS tunneling.
- Highlight the significance of security protocols like DoT and DoH.
- Overview of machine learning and XAI techniques for detecting DNS tunneling.
- Keywords: DNS, Tunneling, DoH, ML, XAI.

## Section II: Introduction

- DNS as a hierarchical system converting domain names to IPs.
- Security challenges in traditional DNS (cache poisoning, MITM attacks).
- Emergence of DNSSEC and its role in bolstering DNS security.
- Overview of DNS tunneling as a covert threat.
- Importance of encryption and associated challenges (e.g., DoH complicating detection).

## Section III: Background

- DNS architecture: root zone, TLDs, resource records, authoritative and recursive servers.
- Detailed discussion on DNSSEC's role, ZSKs, and KSKs for trust chains.
- Limitations of DNSSEC (key management, compatibility).
- Recursive DNS resolution process ensuring user-to-server communication security.
- Challenges posed by DNS vulnerabilities.

## Section IV: State-of-the-Art

- Definition and mechanics of DNS tunneling.
- Role of DNS tunneling in data exfiltration, botnet control, and malware distribution.
- Impact of DoH on detecting DNS-based threats:
- Modern detection techniques
- Explainable AI (XAI) approaches for enhancing transparency in detection.

## Section V: Conclusion

- Recap of DNS’s importance and vulnerabilities.
- Challenges and advantages of encryption technologies (DoH, DNSSEC).
- Critical need for multilayered security frameworks.
- Role of ML and XAI in advancing detection and mitigation.
- Call for continuous research to address evolving DNS-related cyber threats.

REFERENCES

[1] F. Zou, S. Zhang, B. Pei, L. Pan, L. Li and J. Li, "Survey on Domain Name System Security," *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, Changsha, China, 2016, pp. 602-607, doi: 10.1109/DSC.2016.96.

[2] IETF. RFC 1035 Domain Names - Implementation and Specification[DB/OL]. 1987-11[2011-8-16] http://www.ietf.org/rfc/rfc1035.txt.

[3] IETF. RFC 4033 DNS Security Introduction and Requirements[DB/OL]. 2005-3[2012-3-21] http://www.ietf.org/rfc/rfc4033.txt.

[4] G. Gürsoy, A. Varol and A. Nasab, "DNS Tunnel Problem In Cybersecurity," *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA, 2024, pp. 1-6, doi: 10.1109/ISDFS60797.2024.10527301.

[5] T. Zebin, S. Rezvy and Y. Luo, "An Explainable AI-Based Intrusion Detection System for DNS Over HTTPS (DoH) Attacks," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2339-2349, 2022, doi: 10.1109/TIFS.2022.3183390.

[6] S. K. Singh and P. K. Roy, "Detecting Malicious DNS over HTTPS Traffic Using Machine Learning," *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Sakheer, Bahrain, 2020, pp. 1-6, doi: 10.1109/3ICT51146.2020.9312004.

[7] N. Ishikura, D. Kondo, V. Vassiliades, I. Iordanov and H. Tode, "DNS Tunneling Detection by Cache-Property-Aware Features," in *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1203-1217, June 2021, doi: 10.1109/TNSM.2021.3078428.