Poster: Reconsidering DNS-Based Domain Verification: Privacy and Overhead Implications

Eunbee Hwang
Seoul National University
Seoul, Republic of Korea
eunbee.hwang@snu.ac.kr

Hyunsoo Kim
Seoul National University
Seoul, Republic of Korea
wayles@snu.ac.kr

Taekyoung Kwon
Seoul National University
Seoul, Republic of Korea
tkkwon@snu.ac.kr

Abstract

Domain verification (DV) using DNS TXT records has become an essential mechanism for proving domain ownership across various online services. However, this practice inadvertently discloses sensitive business relations, increases DNS response sizes, and burdens DNS resolver infrastructures. Our measurement of over 2.5 million DNS TXT records highlights the prevalence of bloated TXT records. This work serves as a preliminary problem statement motivating privacy-preserving and efficient DV mechanisms.

CCS Concepts

• **Networks** → **Application layer protocols**; • **Security and privacy** → **Network security**.

Keywords

DNS, Domain Verification, Privacy, Measurement

ACM Reference Format:
Eunbee Hwang, Hyunsoo Kim, and Taekyoung Kwon. 2025. Poster: Reconsidering DNS-Based Domain Verification: Privacy and Overhead Implications. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3719027.3760724

1 Introduction

The Domain Name System (DNS) continues to grow in both scale and significance. The volume of DNS queries and the number of registered domains are steadily increasing. For example, Cloudflare's public resolver 1.1.1.1 now processes approximately 1.9 trillion queries per day worldwide [1]. At the same time, DNS response sizes have also been rising [2], driven in part by the adoption of IPv6, deployment of DNSSEC, encrypted DNS protocols such as DNS-over-TLS and DNS-over-HTTPS, and the proliferation of diverse record types.

One of the key contributors to this increase is the widespread use of DNS TXT records. While it was originally intended as flexible, free-form text records, they have become the standard mechanism for publishing machine-readable tokens for domain verification and email authentication (e.g., SPF, DKIM, DMARC) [4, 7].

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3760724

This paper focuses on domain verification (DV), a critical process when an entity—such as a company or organization—subscribes to an online service using its own domain name. As illustrated in Figure 1, DV typically involves the service provider issuing a unique verification token, which the entity publishes as a DNS TXT record to demonstrate control over the domain. DV is widely used across several categories of services. For example, cloud service providers rely on DV to enable features such as email, collaboration, and infrastructure hosting. Similarly, Certificate Authorities (CAs) are required to perform DV before issuing TLS certificates to domain owners.

Table 1 shows the examples of DV TXT records used by major service providers. It highlights not only the prevalence of each provider's records but also whether the verification is a one-time process or requires periodic checks for continuous verification, in which case the TXT record must remain in place as long as the service is active. Comparing our measurements and those from 2019 [5] shows that the use of DV TXT records has grown substantially over the past six years. For example, among the top 1 million domains, `google-site-verification` records alone increased almost fourfold from 2019 to 2025.

This paper highlights the privacy and operational risks arising from this trend. We provide a large scale measurement-based analysis of DV TXT records, discuss their security and performance implications, and suggest potential approaches to mitigate these challenges.

2 Security and Performance Implications

Domain owners increasingly add multiple domain verification tokens to their DNS configurations. While this DNS-based domain verification is convenient, we believe it can introduce security, privacy, and performance issues.

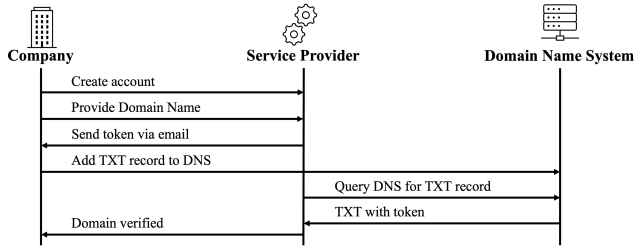

Figure 1: The DV process is illustrated, where the service provider issues a token that the subscriber publishes as a DNS TXT record to prove the ownership of its domain name.

Provider	Domain Verification Record	Category	Verification	# of records [5]	# of records ('25)
Google	`google-site-verification=MXbDGi8. . .`	Cloud Services	Periodic	149,785	595,105
Microsoft	`MS=ms62662176`	Cloud Services	Once	70,797	192,384
Facebook	`facebook-domain-verification=v6n. . .`	Cloud Services	Periodic	16,028	77,537
Globalsign	`_globalsign-domain-verification=. . .`	Certificate Authority	Once	11,486	56,965
Adobe	`adobe-idp-site-verification=ffe3. . .`	Electronic Signing Cloud Services	Once	5,097	15,660

Table 1: Examples of DV TXT records used by major service providers, including their category, verification type, and the number of records observed in 2019 [5] and in our measurements.

2.1 Information Leakage and Privacy

A TXT record for DV usually corresponds to a particular third-party online service such as Google services and Microsoft Office 365. When domain owners leave these tokens in DNS, anyone can retrieve these TXT records, which inadvertently reveals which services or platforms the domain subscribes to.

This privacy implication means that DV TXT records can be abused by attackers, who can profile the domain owner's online services. Such information can be utilized for supply-chain attacks or tailored phishing [5]. Attackers may look for services that support federated authentication without multi-factor authentication (MFA), such as Office 365 and G Suite, in order to attempt credential-based access to cloud resources. Adversaries can infer details about the domain owner's security—such as whether they rely on CDNs to distribute and protect their website content, which email protection services/3rd party marketing and analytics they use. It can also reveal which CA issues its TLS certificates. In other words, the convenience of DV comes at the cost of exposing the domain's relations to external services.

2.2 Increased Latency and Resolver Overhead

A domain with many DV TXT records will often return a bloated DNS response. DNS was originally designed to operate over UDP, with a typical size limit of 512 bytes. When responses exceed these limits, they are truncated, resulting in a fallback of DNS over TCP. Measurements show that the ratio of DNS queries that fall back to DNS-over-TCP sessions not negligible, which will consume substantial CPU and memory resources [8].

Public DNS resolvers can typically absorb this overhead using large-scale anycast networks, extensive caching, and robust load balancing. In contrast, private or smaller resolvers often lack such infrastructures. Repeated queries—particularly for domains with numerous TXT records—can lead to cache evictions, increased latency, and higher failure rates, especially when multiple clients trigger frequent TCP fallbacks. In these environments, large responses may impose excessive load, degrading the resolver's overall performance and reliability.

Transitioning from UDP to TCP for DNS has broader user implications. When TCP fallback occurs, clients must establish new connections and resend queries, introducing additional latency and traffic. Even in well-provisioned networks, this adds overhead. Moreover, multiple TXT records significantly increase response sizes—TXT-based verification tokens are a major contributor to DNS response bloat [6].

2.3 DNS Amplification Attack Vector

The presence of numerous TXT records can be exploited in DNS amplification attacks. In such distributed denial-of-service (DDoS) attacks, an adversary sends a small DNS query—typically for TXT records—while spoofing the victim's IP address. This causes the DNS server to send a large response to the victim, overwhelming their machine or network. When a domain accumulates many DV TXT records, it inadvertently creates a scenario where a lightweight query triggers a large response. Prior research has shown that attackers have exploited oversized DNS responses for amplification [7]. This suggests that the common practice of stacking DV TXT records is not only inefficient in terms of space but also poses a tangible security risk.

3 DV TXT Records Measurement

3.1 Domain List and TXT Records in General

We collected a total of 2,548,194 TXT records based on the Tranco Top 1M domain list [3]. Among these domains, approximately 270k had no TXT records at all. For the remaining domains that have at least one TXT record, we observed an average of 3.49 TXT records per domain. When focusing on the Top 10k domains, only 1,495 domains lacked any TXT records, and those with at least one record have an average of 8.17 TXT records. This disparity indicates that more popular and frequently visited domains tend to have more TXT records (or subscribed with more online service providers), including domain verification and email authentication.

3.2 DV TXT Records

To identify TXT records for DV, we develop a program for regular expressions that find matching prefixes defined by service providers, such as `google-site-verification=` and `MS=`. These records typically start with such identifiers, followed by special characters like `=`, `-`, or `:`, and then a random token string. Using these patterns, we find out that out of the 2,548,194 collected TXT records, 1,460,642 (approximately 57%) are for DV. When limiting the analysis to the 485,790 domains that have at least one DV TXT record, the average count is 3.01 per domain. As mentioned before, domains with higher web traffic tend to have more DV TXT records. As shown in Figure 2, nearly 70% of the Top 10k domains contained at least one DV TXT record, highlighting the strong correlation between web prominence and the use of such DV mechanisms. Among all observed domains, `aveanna.com` and `gvsu.edu` have the highest counts of DV TXT records, each exceeding 170 entries.

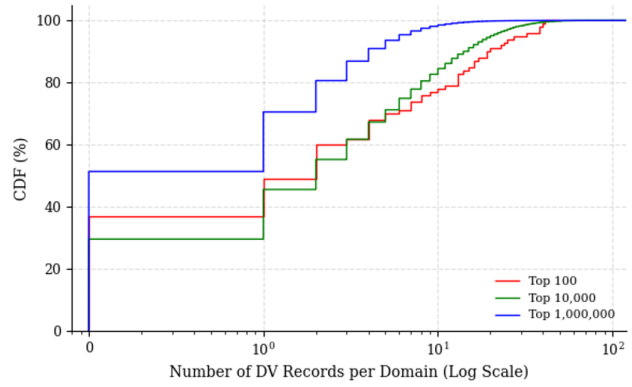

Figure 2: The cumulative distribution of DV TXT record counts per domain is shown on a logarithmic scale.

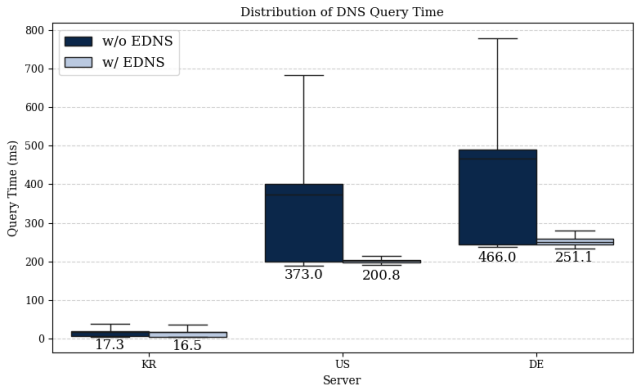

Figure 3: The distribution of DNS query delays when fetching DV TXT records from authoritative servers in KR, US, and DE, with and without EDNS enabled.

3.3 Fetching DV TXT Records

To measure the delay experienced by online service providers when retrieving DV TXT records, we deployed authoritative nameserver instances on cloud platforms in South Korea, the United States, and Germany. For each region, we sequentially loaded zone files containing the TXT records of the Top 10k domains. We then set up a measurement server and a private DNS resolver located in South Korea to emulate a service provider querying these records. When the EDNS option is disabled, DNS responses for 3,530 domains are too large to fit in a single UDP packet, triggering TCP fallback. In contrast, enabling EDNS reduced the number of such cases to only 45 domains. As illustrated in Figure 3, the additional round-trip time (RTT) incurred by TCP fallback is substantial. For nameservers located farther from the measurement node (e.g., in the US and Germany), the retrieval time increased by an average factor of 1.8 or more depending on EDNS usage. This observation suggests that if DV TXT records are instead delegated to dedicated selectors (`_google-domain-verification.example.com`) rather than published directly at the apex domain (`example.com`), it would be possible to reduce the bandwidth consumption and latency.

4 Conclusion

This preliminary study shows that DNS-based domain verification (DV), while convenient and widely adopted, introduces notable privacy risks and operational inefficiencies. Delegating verification tokens to subdomains using selectors, rather than placing them at the apex domain, appears promising for mitigating DNS bloat and reducing the risk of inference attacks. We are developing a method that leverages probabilistic data structures for DV, aiming to streamline resolver operations while preserving domain owner privacy. Future work will focus on balancing usability, privacy, and performance to support safer and more efficient DV practices.

Acknowledgments

This work was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-2021-0-02048) supervised by the IITP (Institute for Information Communications Technology Planning Evaluation), IITP grant funded by the Korea government (MSIT) [NO.RS-2021-II211343, AI Graduate School Program (Seoul National University)], and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2022R1A2C2011221, No. RS-2023-00220985), and also supported by Basic Science Research Program through the NRF funded by the Ministry of Education (RS-2024-00354503).

References

[1] David Belson, Carlos Rodrigues, Vicky Shrestha, and Hannes Gerhart. 2025. *Some txt about, and a PTR to, new DNS insights on Cloudflare Radar.* Retrieved July 11, 2025 from https://blog.cloudflare.com/new-dns-section-on-cloudflare-radar/#:~:text=No%20joke%20%E2%80%93%20Cloudflare%27s%201,1%20data%20to

[2] Mike Kosek, Trinh Viet Doan, Simon Huber, and Vaibhav Bajpai. 2022. Measuring DNS over TCP in the Era of increasing DNS Response Sizes: A View from the Edge. *ACM SIGCOMM Computer Communication Review* 52, 2 (2022), 44–55.

[3] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019).* doi:10.14722/ndss.2019.23386

[4] Adam Portier, Henry Carter, and Charles Lever. 2019. Security in plain txt: Observing the use of dns txt records in the wild. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19–20, 2019, Proceedings 16.* Springer, 374–395.

[5] Scott Sutherland. 2019. *Analyzing DNS TXT Records to fingerprint online service providers.* Retrieved July 11, 2025 from https://www.netspi.com/blog/technical-blog/network-pentesting/analyzing-dns-txt-records-to-fingerprint-service-providers/

[6] Olivier van der Toorn, Johannes Krupp, Mattijs Jonker, Roland van Rijswijk-Deij, Christian Rossow, and Anna Sperotto. 2021. ANYway: measuring the amplification DDoS potential of domains. In *2021 17th International Conference on Network and Service Management (CNSM).* IEEE, 500–508.

[7] Olivier Van Der Toorn, Roland van Rijswijk-Deij, Tobias Fiebig, Martina Lindorfer, and Anna Sperotto. 2020. TXTing 101: finding security issues in the long tail of DNS TXT records. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).* IEEE, 544–549.

[8] Jan Věelák. 2017. *DNS over TCP as seen from the authoritative servers.* Retrieved July 11, 2025 from https://indico.dns-oarc.net/event/26/contributions/442/attachments/404/685/vcelak_dns_over_tcp.pdf

Received 11 July 2025; accepted 4 August 2025