IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4636425/
Vol. 2025 (37), Article ID 4636425

Domain Name System threats and Role of DNSSEC in Security*

Piotr KONTOWICZ

Poznan University of Technology, Faculty of Computing and Telecommunications,

Piotrowo 3, 60-965 Poznan, Poland

Correspondence should be addressed to: Piotr KONTOWICZ, piotr.kontowicz@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The Domain Name System (DNS) is a fundamental component of Internet infrastructure. Its original design lacked mechanisms for data security and authenticity. Consequently, DNS remains vulnerable to various attacks. In recent years, these attacks have evolved from basic response spoofing to sophisticated campaigns, including distributed denial-of-service (DDoS) and amplification attacks, data integrity breaches such as DNS cache poisoning and DNS hijacking, as well as communication tunneling.

This paper classifies DNS threats according to the confidentiality, integrity, and availability (CIA) triad, demonstrating how attackers exploit protocol vulnerabilities to redirect users, exfiltrate data, or disrupt services. In response, Domain Name System Security Extensions (DNSSEC) were introduced to provide data integrity and authenticity through cryptographic signatures. However, DNSSEC does not ensure confidentiality or comprehensive infrastructure protection. Additional protocols, including DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH), encrypt DNS communication but complicate traffic analysis and threat detection. The Response Policy Zone (RPZ) mechanism further enhances defense by blocking access to malicious domains, though its effectiveness is reduced when DNS traffic is encrypted.

No single security mechanism offers comprehensive protection for DNS. Implementing a multilayered security model that integrates multiple technologies is essential to balance confidentiality, integrity, and availability. Current research is directed toward incorporating post-quantum cryptography to address emerging threats associated with quantum computing.

Keywords: DNS, DNS Security, DNS Attacks, DNSSEC, DoT, DoH, DNS Cache Poisoning, DNS Amplification, DNS Tunneling, RPZ, CIA Triad

Introduction

The Domain Name System (DNS) underpins Internet functionality by translating domain names into IP addresses. The original DNS protocol lacked security mechanisms to verify the authenticity of server responses, enabling attackers to redirect users to fraudulent websites. Present-day DNS threats extend beyond basic attacks. This paper categorizes these threats into three groups: distributed denial-of-service (DDoS) and volumetric attacks, integrity violations, and communication tunneling.

To address emerging threats, Domain Name System Security Extensions (DNSSEC) were introduced with an emphasis on ensuring data integrity. DNSSEC forms a critical component of a comprehensive security strategy, which should also incorporate supplementary mechanisms to defend against advanced attacks. This approach is particularly vital in sectors demanding high levels of trust.

Cite this Article as: Piotr KONTOWICZ, Vol. 2025 (37) "Domain Name System threats and Role of DNSSEC in Security " Communications of International Proceedings, Vol. 2025 (37), Article ID 4636425, https://doi.org/10.5171/2025.4636425

Because DNSSEC does not provide confidentiality, additional mechanisms such as DNS-over-TLS (DoT) or DNS-over-HTTPS (DoH) must be implemented in environments where user privacy is essential.

Categories of DNS attacks

Attacks on DNS infrastructure can be systematically categorized according to the confidentiality, integrity, and availability (CIA) triad. Classifying threats by their primary objectives compromising confidentiality, integrity, availability, or resulting from infrastructure takeover enables structured analysis of their impact.

DNS Integrity

One of the attacks targeting data integrity is DNS cache poisoning. This attack involves injecting forged DNS records into the server's cache [2]. The attacker sends spoofed DNS responses to the resolver in order to store false IP addresses for a given domain in its cache. Once the malicious records are cached, the domain becomes poisoned. Since the cache is the first place checked when a new query is made, subsequent requests for the affected domain are directed to the incorrect IP address. As a result, users querying the DNS server are redirected to services controlled by the attacker.

DNS hijacking is another attack that compromises DNS integrity. Attackers, after gaining access to a domain administrator's account, can modify the IP address configured for the domain. This attack can also be carried out using malicious software installed on the victim's device. Such malware can alter local DNS settings to redirect traffic to harmful websites. Attackers may also exploit vulnerabilities in users' home routers. Examples of such vulnerabilities include default passwords or outdated firmware with known security flaws that allow remote access.

Another attack frequently mentioned in reports is DNS pharming. In its simplest form, it involves modifying the HOSTS file on the victim's device. In more advanced scenarios, it may involve changing the victim's router settings. The HOSTS file is used for local domain name resolution, and its modification can lead to users being redirected to attacker-controlled websites.

Attacks compromising DNS integrity may result in the theft of authentication credentials or facilitate malware distribution. These attacks are particularly hazardous due to their potential to impact numerous users simultaneously. Attackers often employ such methods for large-scale phishing campaigns, traffic censorship, or unauthorized collection of browsing information.

Attacks on availability

Distributed denial-of-service (DDoS) and volumetric attacks primarily target the availability of DNS services. The objective of these attacks is to exhaust server resources, computing power, and network bandwidth, rendering the server incapable of processing legitimate user requests.

The first example of such an attack is an amplification attack [3], which consists of several stages. The initial step involves source address spoofing, where the attacker uses IP spoofing to falsify the source IP address in a packet, replacing it with the IP address of the victim. This spoofed request is then sent to open DNS servers. These are often ANY-type queries, which request all available records for a given domain and generate a much larger response than the original query.

The DNS server then sends the large response to the forged IP address the victim's address making it appear as though multiple servers are simultaneously sending large amounts of data to the target. The attacker, leveraging many sources such as a botnet, sends parallel queries to hundreds or thousands of servers. Since each query can generate a response many times larger than the request, the traffic quickly saturates the victim's bandwidth and server resources.

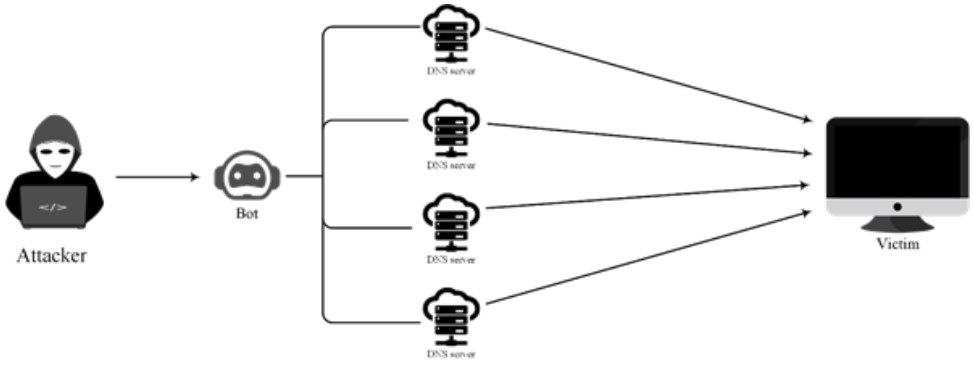

Figure 1. DNS amplification attack

Another type of attack is the DNS flood attack, in which attackers use a botnet to generate a high volume of DNS queries with the goal of exhausting network bandwidth or server resources. As a result of this activity, legitimate users are denied service, and from their perspective, it appears that their queries are not being properly handled, giving the impression that the application is unavailable.

Servers may also be flooded with DNS queries for non-existent or hard-to-resolve domains. This attack is known as an NX Domain Attack or Random Subdomain Attack, as it may involve queries for random subdomains. DNS servers must process every received query and return an NXDOMAIN error response. This can lead to delayed responses from the target server. The attack typically results in a high rate of NXDOMAIN responses and is sometimes misinterpreted as a performance issue within the system.

Typical consequences of this category of attacks include service overload and unavailability. Due to the exhaustion of bandwidth and server resources, websites and services may become partially or entirely inaccessible. Service outages can lead to lost orders, which directly translate into financial losses. Prolonged availability issues also undermine customer trust and negatively affect a company's reputation.

Tunneling of communication

The DNS protocol can also be used for communication tunneling, which violates the confidentiality property of data. Such attacks leverage legitimate network protocols to conceal communication. DNS is commonly used in these attacks because it is typically allowed and considered a trusted protocol.

DNS tunneling is a technique that abuses the DNS protocol to hide communication between a victim’s system and an attacker's system. In this method, DNS queries and responses are used as a data transmission channel. The transmitted data may include sensitive internal company information or content related to malware operating on infected machines. Malicious software often communicates with command-and-control servers while concealing its nature by embedding it within legitimate protocols.

Attackers typically embed data in DNS query subdomains, which are additionally encoded to obscure the presence of covert communication, making detection during event analysis more difficult. The command server usually communicates with the malware using TXT records or other rarely used DNS fields. This attack is effective because DNS traffic is often allowed through firewalls and treated as trustworthy, even in highly controlled environments.

As highlighted by Palo Alto Networks [4], this technique is commonly used in espionage campaigns and is also employed for data exfiltration and maintaining communication between infected hosts and Command and Control (C2) infrastructure.

DNS rebinding is another attack that allows attackers to gain control over locally running web applications. By leveraging the properties of the DNS system, an attacker can bypass the Same-Origin Policy enforced by web browsers. The attacker registers a domain under their control, which initially resolves to an attacker-controlled server. After a short period (with a deliberately low time-to-live value for the DNS record), the address is changed to an internal IP address within the victim’s network. This enables malicious scripts embedded in the user's browser to issue HTTP requests to local resources, bypassing browser security mechanisms and firewalls.

Detecting communication tunneling attacks is a complex task that requires advanced analysis. One factor that further complicates the detection of covert DNS-based communication is the encryption of DNS traffic.

DNSSEC as part of a multilayer defense approach

Domain Name System Security Extensions *(DNSSEC)* extend the DNS protocol by introducing security mechanisms that ensure the authenticity and integrity of information about Internet addresses.

DNSSEC is a set of extensions to the DNS protocol that guarantees the authenticity and integrity of responses. This property is achieved through the use of public key cryptography to digitally sign DNS records, creating a chain of trust from the root zone to other DNS servers. The mechanism effectively addresses issues related to the integrity of DNS entries; however, it has certain limitations:

1. lack of confidentiality: DNSSEC queries are still transmitted in plaintext.
2. limited protection: the protocol does not provide defense against attacks on the infrastructure or registrar account takeovers.
3. last-mile problem: validation usually ends at the first DNS server from the user's perspective, typically the isp's resolver. man-in-the-middle attacks at the local network level are still possible.

DNSSEC addresses data integrity concerns but does not provide communication confidentiality. Achieving confidentiality requires the deployment of supplementary security mechanisms.

DNS Traffic Encryption – Ensuring Confidentiality

To ensure confidentiality, the DNS-over-TLS (DoT) [5] and DNS-over-HTTPS (DoH) [6] protocols were developed. DoT encrypts DNS traffic using the TLS protocol and operates on a dedicated port 853. Due to the use of a unique port, its presence can be identified and monitored by network administrators, while still maintaining user confidentiality.

DoH encapsulates DNS traffic within HTTPS and uses port 443, which makes this traffic indistinguishable from regular web browsing. From an administrator's perspective, DoH presents a challenge, as it is not possible to differentiate related traffic, nor can connections to unauthorized DNS servers be easily monitored or blocked.
Given these challenges, DNS-over-TLS (DoT) is generally preferred because it permits monitoring of traffic volume, even though the content remains encrypted.

Filtering Using DNS Response Policy Zones (RPZ)

One of the defense mechanisms for devices operating within a local network is blocking connections to known malicious domains. This mechanism is implemented using DNS Response Policy Zone (RPZ) [7]. Lists of such domains, often referred to as threat intelligence feeds, are regularly updated by specialized organizations such as Cisco, Palo Alto, CISA, and Google. Administrators can configure a DNS server to either prevent responses to queries for blacklisted domains or to return a warning message to the user.

This approach serves as an effective defense against malware infections. When properly configured, it blocks communication with servers controlled by cybercriminals, thereby significantly impeding malicious operations.
A major challenge in configuring and deploying this solution is the use of DoH and DoT. When DNS queries are transmitted through encrypted communication channels, filtering mechanisms cannot function properly. It becomes impossible to inspect the contents of DNS packets, determine the queried domain, or compare it against deny lists.

This situation creates a paradox: enhancing user privacy may inadvertently increase exposure to threats by permitting communication with attacker-controlled servers. Deploying an internal DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) server is the only effective mitigation.

Conclusion

DNS-related threats have progressed from basic response spoofing to advanced infrastructure attacks and covert communication techniques. In the current threat landscape, a single security mechanism is insufficient, as no individual solution ensures confidentiality, integrity, and availability. A multilayered security model that integrates multiple mechanisms is necessary to achieve comprehensive protection.

For businesses and organizations, balancing user privacy with corporate security presents a significant challenge. Achieving both objectives simultaneously is complex. Implementing encryption to enhance user privacy complicates traffic filtering and detection of connections to attacker-controlled command servers.

A further challenge for both security and performance is the emergence of threats linked to the development of quantum computing. The advancement of such technologies could eventually break the encryption currently used in DoH and DoT, as well as the digital signatures in DNSSEC. Ongoing research is focused on adapting post-quantum cryptography (PQC) [8] to secure the protocol in a future where sufficiently powerful quantum computers could compromise today's cryptographic algorithms. One of the major challenges in this transformation is ensuring the performance efficiency of post-quantum algorithms [9], so that the encryption of queries and responses does not introduce excessive computational overhead.

Acknowledgements

This research was funded by the Polish Ministry of Science and Higher Education under Grant 0313/SBAD/1311.

Bibliography

- R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, DNS Security Introduction and Requirements, RFC 4033, Mar. 2005.
- D. Kaminsky, "Black Ops 2008: It's The End Of The Cache As We Know It," presented on Black Hat USA 2008, Las Vegas, NV, Aug. 2008.
- P. Vixie, "DNS Amplification Attacks," SANS Institute, 2002.
- Palo Alto Networks Unit 42, "DNS Tunneling: Hiding in Plain Sight," 2017.
- Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, Specification for DNS over Transport Layer Security (TLS), RFC 7858, May 2016.
- P. Hoffman and P. McManus, DNS Queries over HTTPS (DoH), RFC 8484, Oct. 2018.
- P. Vixie and R. Schryver, DNS Response Policy Zones (RPZ), Internet Systems Consortium (ISC), 2010.
- National Institute of Standards and Technology (NIST), Post-Quantum Cryptography (PQC), 2022.
- P. Hoffman, "Algorithm Agility in DNSSEC," Internet-Draft, IETF, 2023.