Poster: TuDoor Attack
Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

Xiang Li[‖¶], Lu Sun[‖], Wei Xu[¶], Baojun Liu[¶], Mingming Zhang[‡¶], Zhou Li[†✉], Jia Zhang[¶‡], Deliang Chang[£], Xiaofeng Zheng[¶£], Chuhan Wang[$¶], Jianjun Chen[¶‡], Haixin Duan[¶‡$✉], and Qi Li[¶✉]

[‖]Nankai University, [¶]Tsinghua University, [†]University of California, Irvine
[‡]Zhongguancun Laboratory, [$]Quan Cheng Laboratory
[£]QI-ANXIN Technology Research Institute, [$]Southeast University
✉Corresponding Author(s)

Abstract

DNS can be compared to a game of chess in that its rules are simple, yet the possibilities it presents are endless. While the fundamental rules of DNS are straightforward, DNS implementations can be extremely complex. In this study, we intend to explore the complexities and vulnerabilities in DNS response pre-processing by systematically analyzing DNS RFCs and DNS software implementations. We present the discovery of three new types of logic vulnerabilities, leading to the proposal of three novel attacks, namely the TuDoor attack. These attacks involve the use of malformed DNS response packets to carry out DNS cache poisoning, denial-of-service, and resource consuming attacks. By performing comprehensive experiments, we demonstrate the attack's feasibility and significant real-world impacts of TuDoor. In total, 24 mainstream DNS software, including BIND, PowerDNS, and Microsoft DNS, are affected by TuDoor. Attackers can instigate cache poisoning and denial-of-service attacks against vulnerable resolvers using a handful of crafted packets within 1 second or circumvent the query limit to deplete resolution resources (e.g., CPU). Besides, to determine the vulnerable resolver population in the wild, we collect and evaluate 16 popular Wi-Fi routers, 6 prevalent router OSes, 42 public DNS services, and around 1.8M open DNS resolvers. Our measurement results indicate that TuDoor could exploit 7 routers (OSes), 18 public DNS services, and 424,652 (23.1%) open DNS resolvers. Following the best practice of responsible disclosure, we have reported these vulnerabilities to all affected vendors, and 18 of them, including BIND, Chrome, Cloudflare, and Microsoft, have acknowledged our findings and discussed mitigation solutions with us. Furthermore, 33 CVE IDs are assigned to our discovered vulnerabilities, and we provide an online detection tool as one of the mitigation measures. Our research highlights the urgent need for standardization of DNS response pre-processing logic to enhance the security of DNS.

Acknowledgment

This work [1] was published in the Proceeding of 2024 IEEE Symposium on Security and Privacy (IEEE S&P 2024).

The full bibliographic reference is listed below.

The authors of this poster are shown above[1].

The original abstract is shown above.

The link to this paper is https://ieeexplore.ieee.org/document/10646751.

This paper was also presented at Black Hat USA 2024.

References

[1] Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, Deliang Chang, Xiaofeng Zheng, Chuhan Wang, Jianjun Chen, Haixin Duan, and Qi Li. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In Proceedings of 2024 IEEE Symposium on Security and Privacy, IEEE S&P '24, 2024.

1. Lu Sun contributed to the preparation and presentation of the poster but is not an author of the original paper.

Poster: TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

Xiang Li [1 2] Lu Sun [1] Wei Xu [2] Baojun Liu [2] Mingming Zhang [4 2] Zhou Li [3]
Jia Zhang [2 4] Deliang Chang [6] Xiaofeng Zheng [2 6] Chuhan Wang [7 2]
Jianjun Chen [2 4] Haixin Duan [2 4 5] Qi Li [2]

[1] Nankai University [2] Tsinghua University [3] University of California, Irvine [4] Zhongguancun Laboratory
[5] Quan Cheng Laboratory [6] QI-ANXIN Technology Research Institute [7] Southeast University

DNS Resolution and Packet

- Translate human-friendly domain names into machine-readable IP addresses and vice versa.
- **Multiple resolver roles:** stub, forwarder, recursive, and authoritative.
- **Iterative resolution process:** C/S style, recursive resolution, and caching.

Figure 1. General DNS resolver roles and domain name resolution process.

- Communicating primarily over **UDP**.
- **DNS packet:** a 12-byte DNS header and a DNS body.
- **Two important fields:** `TxID` for authentication and `QR` indicating a query (0) or response (1).

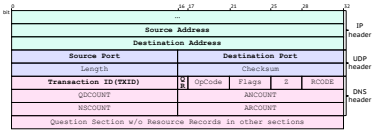

Figure 2. DNS packet format on UDP.

DNS Cache Poisoning Attacks

- **Injecting forged responses** into resolvers' cache and hijacking domains and traffic.
- DNS cache poisoning attacks **continue to be proposed** after multiple mitigation solutions.

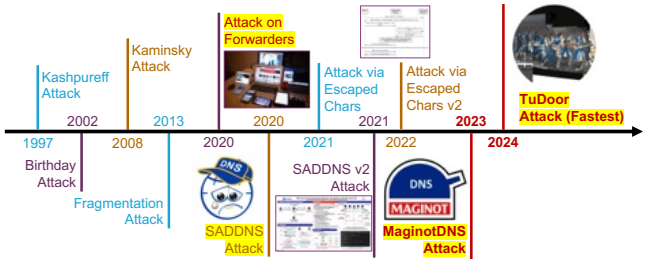

Figure 3. Timeline of DNS cache poisoning attacks.

TuDoor Attack [1]

- New powerful **DNS-related attacks**: cache poisoning, DoS, and resource consuming.
- **TuDoor in the DNS Wall:** a very covert side-channel like 突门 in the Great Wall.
- **Exploiting vulnerabilities** in **DNS response Pre-processing** with malformed packets.

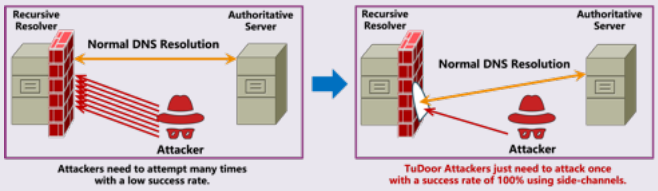

Figure 4. TuDoor attack model.

Analysis of DNS Response Pre-processing

- DNS response pre-processing **never been studied** thoroughly, leaving potential threats.
- **What we did:** constructing **state machines** for response pre-processing and finding bugs.

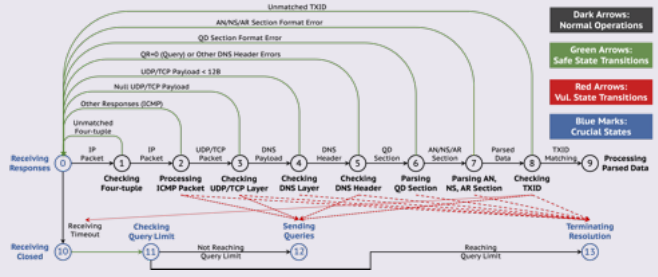

Figure 5. General state machine model of DNS response pre-processing (Except for the red dotted arrows).

Vulnerable State Transitions

- **28 DNS software:** 8 recursive, 10 forwarders, 6 stub, and 4 DNS libraries (**24 vulnerable**).

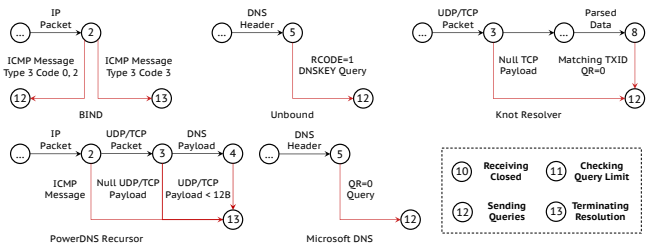

Figure 6. Part of vulnerable state transitions with red lines.

TuDoor Attack Example (1/3): DNS Cache Poisoning

- Exploiting one **new side-channel vulnerability** to locate the source port with 2,500 packets and brute-force 65,536 TxIDs (The **fastest DNS cache poisoning attack** on Microsoft DNS).
- **Attack time:** avg. 425ms, 200 — 1,000 times **faster** than prior attacks under the same conditions.

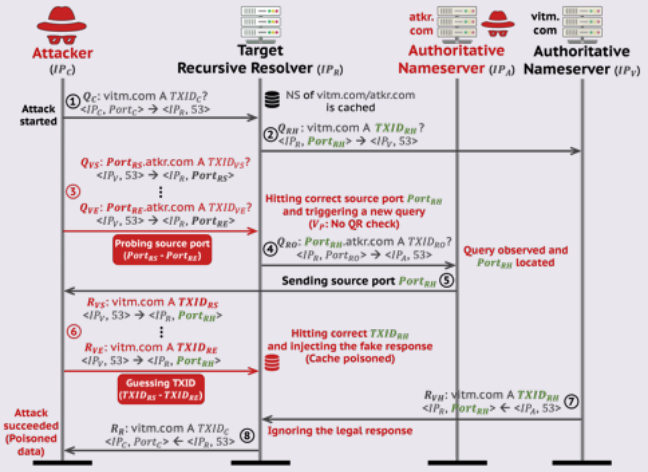

Figure 7. Attack steps of DNS cache poisoning.

Vulnerable Population and Mitigation Solution

- **Vulnerable:** 24/28 DNS software, 18/42 public services, and **423k (23.1%)** open resolvers.
- **Mitigation:** improving poor DNS response pre-processing implementations.
- **Disclosure:** **14 vendors** confirmed TuDoor with **33 CVEs** assigned.
- **Detection & online tool:** https://test.tudoor.net.

Figure 8. Part of vulnerable DNS vendors.

References

[1] Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, Deliang Chang, Xiaofeng Zheng, Chuhan Wang, Jianjun Chen, Haixin Duan, and Qi Li. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In *Proceedings of 2024 IEEE Symposium on Security and Privacy*, IEEE S&P '24, 2024.