Poster: DNS in Routers Considered Harmful

Haya Shulman
ATHENE & Goethe-Universität Frankfurt & Fraunhofer SIT

Michael Waidner
ATHENE & TU Darmstadt & Fraunhofer SIT

ABSTRACT

To save costs residential routers often do not implement most of the functionalities and security features of DNS, yet they still contain DNS forwarders which merely proxy the clients' requests to another address. These forwarders separate the network configuration of the internal client network from the network of the ISP. This provides connectivity without the need for synchronization. History of cache poisoning attacks shows however that such simplified implementations expose a wide range of vulnerabilities. We propose to remove DNS from routers. We show that the performance impact is negligible, while security gain is substantial. We discuss a number of ways for implementing our approach.

CCS CONCEPTS

• **Security and privacy → Network security**.

KEYWORDS

Routers; DNS; Attacks

ACM Reference Format:
Haya Shulman and Michael Waidner. 2022. Poster: DNS in Routers Considered Harmful. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22),November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3548606.3563509

1 INTRODUCTION

Residential routers often implement a DNS component, whose goal is to forward packets between the client devices on the LAN and the upstream resolver, e.g., of an Internet Service Provider (ISP). Such DNS components are also called DNS forwarders. The goal of DNS forwarders in routers is to connect the stub resolvers in client devices to the upstream recursive resolver. The upstream resolver provides full recursive lookup services and also offers caching hence reducing the latency to the client devices. DNS forwarders also themselves often implement a cache hence and store the records from DNS responses of the upstream resolver locally. There is a long history of attacks against the residential routers [1].

Due to their central role, a vulnerability in a DNS forwarder introduces a risk to all the client devices on that LAN. In particular, a DNS cache poisoning attack against a router affects all the clients, redirecting them to incorrect malicious hosts. Recent research demonstrated different techniques for launching DNS cache poisoning attacks against DNS forwarders [2–8].

CCS '22, November 7–11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3563509

Vulnerable third party software. Recently [3] analyzed the factors causing vulnerabilities in DNS forwarders in routers and found that DNS forwarders in the residential routers are often not implemented by routers' developers but by third party software developers and then integrated into the routers. These are however not full fledged DNS resolvers but typically simplified and cheap implementations.

Because of high competition between the routers' vendors over customers the vendors try to offer multiple functionalities while reducing costs to the possible minimum. The need to sell cheap devices leads to minimal investment into the different functionalities. This often results in integration of cheap and often vulnerable third party DNS software into the routers.

DNS vulnerabilities in routers are not trivial to patch. One of the significant problems with vulnerable DNS components in routers is that there is no easy way to patch them. Even when the vendors distribute a patch, this is a patch for the router but not for third party DNS software. On the other hand, when the DNS vendor updates the software, it is not clear how a client can get that update into the router.

R.I.P DNS in routers. In this work we take a unconventional approach at tackling the DNS vulnerabilities in routers: we propose to remove the DNS functionality from the routers. We show that removing the DNS component from routers improves the resilience of home networks and overall of Internet security, without incurring high latency and large traffic volumes. We explain the role of DNS forwarders in routers as well as the primary challenges in our proposal, such as how to find the upstream recursive resolver of the ISP after failures or when clients connect to the network.

No DNS → low overhead. We argue that the cost of our proposal, i.e., the potential increase in latency and traffic due to loss of caching on the routers, is negligible. We explain the benefits that eliminating the DNS in routers promises, including enhanced resilience and security of ISP and client networks by reducing the threats through attacks against DNS in routers.

No DNS → secure routers. Removing the DNS from the routers will resolve the cache poisoning threat and prevent cache poisoning attacks against the clients. In addition, removing DNS will simplify the routers while not requiring any changes to the clients. We show how simple configurations in the ISP DNS infrastructure would enable removing the DNS from the routers.

Organization. We explain the role of DNS forwarders in routers in Section 2. In Section 3 we describe different ways to remove DNS from routers and discuss challenges, hurdles and opportunities. In Section 4 we show that the performance penalty is minimal and acceptable.

2 DNS FORWARDERS IN ROUTERS

In this section we explain how DNS forwarders in residential routers work, and what function they fulfill.

DNS functionality in routers. DNS forwarders in residential routers merely proxy the clients' requests to another address. These

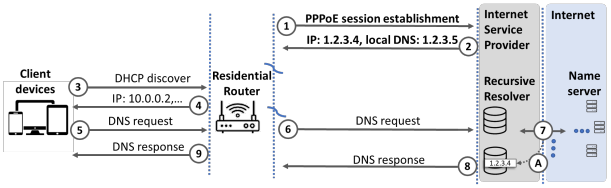

Figure 1: DNS forwarding in routers.

forwarders only separate the network configuration of the internal client network from the network of the ISP. This provides connectivity without the need for synchronization. In a typical DNS forwarder setup on a residential router, the router creates its own internal network segment from an internal network address block, e.g., 10.0.0.0 - 10.255.255.255. The IP addresses of the client devices are allocated from that block. The client devices also receive the IP address (selected from that block) of the basic services, most notably the default gateway and the DNS resolver. All of these addresses are provided to the client devices over a DHCP [RFC2131]. The DNS requests of the stub resolvers on the client applications are sent to the router which forwards them to the upstream resolver, e.g., that of the ISP. The router receives the IP address of the upstream resolver from the ISP over PPPoE [RFC4938] or DHCP [RFC2131]. The resolver of the ISP operates in a recursive mode and answers every query it receives from the internal networks. If the requested query is in the cache, the resolver responds from the cache. Otherwise, the resolver performs a resolution, caches the records from the responses, and forwards the response to the requesting client.

Role of DNS forwarders in routers. [3] illustrated why routers require DNS forwarding functionality and cannot simply hand over the address of the upstream DNS resolver to their clients. In the first step (1), the router establishes an internet connection to the ISP (i.e., via PPPoE) and receives the address configuration from the ISP, containing the instruction to set the DNS server to `198.51.100.34`. In step (2), a client connects to the router's network and requests its address configuration via DHCP. The router provides the configurations and instructs the client to send its DNS requests to the ISP DNS server directly at `198.51.100.34`.

Assume that at some time point the Internet connection is reset and subsequently reestablished in step (3) and assume that the ISP assigns a different network block to the customer, this time configuring the router to send its DNS requests to another DNS resolver at `203.0.113.23`. Similar situation can also occur when a client connects but the Internet connection is not yet available. As a result, the DNS configuration in the DHCP transaction is empty. Following example above, in step (4), the client issues a DNS request to its configured DNS server at `198.51.100.34`. However since the IP address was reconfigured, this server is not reachable anymore. As DHCP does not offer any means to communicate the changed address of the DNS server to the client, the only option to resolve the situation is to reconnect the client to the network.

This example illustrates that routers serve as kind of a synchronization mechanism between the client devices on the LAN and the network of the ISP. A lack of synchronization could lead to problems. However, the synchronization can be solved without DNS in routers. In the next section we list a number of ways to implement this functionality without DNS forwarder in routers.

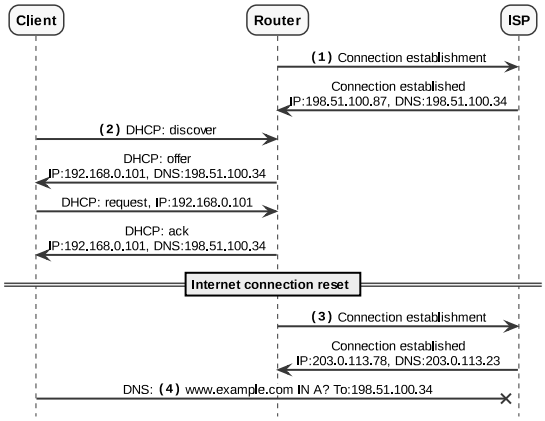

Figure 2: Why routers contain DNS forwarders [3].

Benefits of DNS forwarders. Some DNS forwarder implementations in routers allow clients to configure different settings, like DNS filters, local DNS domains which point to internal IP addresses, enforce additional security protections, like DNS rebinding protection or improve the performance with the help of caching. While such optional features are relevant for some users, and router manufactures might add them for marketing reasons, previous work [3] found that a significant amount of routers which implement DNS forwarders do not implement most of the functionalities and security features of DNS. In addition, the routers were shown to be vulnerable to different kinds of attacks against DNS. The attacks range from injection of records into caches to disabling DNSSEC validation. Consequently, we believe that the ability to support extra features is not worth the risk that the DNS forwarders often expose the client devices to.

Our recommendation to remove DNS applies only to DNS components in routers, as previous studies have shown these are the types of devices most affected by cache poisoning attacks.

3 REMOVING DNS FROM ROUTERS

History shows that DNS is a weak spot in routers. We discuss a different view onto the process of fixing the vulnerabilities in routers While patching specific software bugs or replacing DNS forwarders with more secure implementations presents a fix to some specific vulnerabilities, it does not provide a solution to future vulnerabilities. Our goal is to provide a systematic approach to making routers more secure by removing the dependency of a DNS forwarder in internet gateways. Removing DNS would improve the resilience of routers and client networks, without a significant loss of performance. We propose a number of simple solutions for removing the DNS components from routers. We list three approaches for removing DNS. First is a simple client side configuration. The second is a systematic approach which does not require any actions from the clients. The third is a mechanism for communicating the IP address of DNS resolvers to client devices.

Manually configure upstream resolver. On the client side the users should configure their systems to send queries to an upstream resolver directly, such as the ISP's resolver. This can be accomplished, for instance, by configuring the IP address in the

resolv.conf file to the IP address of the ISP. Using such configurations the clients can bypass the DNS forwarders in routers. The downside of this approach is that it requires the users to configure the IP address of the DNS resolver of the ISP on all the client devices. Every new devices added to the LAN has to be configured. When the ISP changes the DNS resolver to a different IP address, all the client devices need to be reconfigured to send the DNS requests to the correct IP address. If an incorrect IP address is used, the client devices will not be able to access remote services over DNS.

NAT rule to relay requests to upstream. The other approach offers a more systematic method for implementing this, without requiring the clients to change their network configurations. The idea is that instead of implementing a DNS forwarder as a service running on the router's operating system, the routers can implement DNS forwarding as a simple Network Address Translator (NAT) rule. This can be implemented with `iptables` rule. The clients behind the routers are still configured via DHCP to send their DNS requests to the router's internal network address, but these packets are sent directly to the ISP's resolver by rewriting their destination addresses (and potentially also the source ports by the NAT) with a firewall rule. Each time the Internet connection is re-established, e.g., when the router is booted, the firewall rule is changed to route the DNS requests to the correct destination.

Communicate DNS servers to client devices. Another approach to circumvent the problem that routers cannot communicate changing DNS server addresses to clients is to replace the protocol via which this configuration is communicated to the client. Like DHCP, the IPv6 stateless-auto-configuration (SLAAC) mechanism via ICMPv6 router advertisements offers a method of communicating DNS servers to network hosts [RFC8106]. However, in contrast to DHCP, ICMPv6 works statelessly by continuously broadcasting the network configuration in the local network segment. Therefore, this mechanism can be used by routers to communicate a change in DNS resolver configurations to clients which are already connected to the network, and therefore circumvent the synchronization problem illustrated in Fig 2. However, since ICMPv6 is only available for configuration of IPv6 addresses, routers which support IPv4-only clients cannot use this option and must still implement some form of DNS forwarding service.

4 PERFORMANCE COSTS

The routers offer caching to the client devices on a local network, which reduces the latency to the resolver of the ISP. However, the resolvers of the ISPs are located in proximity to client networks and hence latency is anyway limited to milliseconds. Additionally, the resolver of the ISP has a much larger cache, which also includes the records cached on the residential router, therefore the client devices will anyways query the upstream resolver for most records. For records which were recently visited, they are also locally cached: operating systems and applications like browsers also include DNS caches, which makes caching in routers redundant. A record cached in the router will also be included in the cache of the client devices, as well as at the upstream resolver of the ISP.

The analysis of [3] showed that the only performance hit is an increase in page loading times of 1 RTT, measured between the local device and the ISP's resolver, when a DNS record is requested for which there is no cached corresponding record in the local DNS cache, but is present on the router's cache. Since the TTL values of most records are less than 5 minutes, in most cases even with DNS cache in router, the clients still needs to wait for the query to be recursively resolved by the ISP. [3] measured the TTL values of popular A records in Alexa 100K-top domains, and found that 14.066 domains (14%) have a TTL of up to 60 seconds and 53473 (55%) have a TTL under 5 minutes. Consequently, for a router's DNS cache to save the loading time of a typical web-page, the user has to load a page which he has not visited for the last 5 minutes (otherwise the record is locally cached), which was also visited by another device on the same local network less than 5 minutes ago, so that the record is present in the router's cache and has not timed out yet.

5 CONCLUSIONS

Recent work [3] analyzed the factors showing that the vulnerabilities are not individual cases and the problems are prevalent, and can be found in different open and close source implementations. [3] traced the problems to simplified DNS implementations caused by attempts to reduce costs due to high competition between the routers' vendors. Since DNS resolvers are complex systems, with many components, simplification or modification of any of these can lead to vulnerabilities. We review the motivation for using DNS in routers. We discuss removing DNS forwarders from routers and consider the side effects on performance.

ACKNOWLEDGEMENTS

This work has been co-funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) SFB 1119.

REFERENCES

[1] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A {Large-Scale} analysis of the security of embedded firmwares," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 95–110.

[2] K. Schomp, T. Callahan, M. Rabinovich, and M. Allman, "DNS Record Injection Vulnerabilities in Home Routers," 2013. [Online]. Available: https://www.icir.org/mallman/talks/schomp-dns-security-nanog61.pdf

[3] P. Jeitner, H. Shulman, L. Teichmann, and M. Waidner, "XDRI Attacks - and - How to Enhance Resilience of Residential Routers," in *31th USENIX Security Symposium (USENIX Security 22)*, 2022.

[4] K. Schomp, M. Allman, and M. Rabinovich, "Dns resolvers considered harmful," in *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*, 2014, pp. 1–7.

[5] A. Herzberg and H. Shulman, "Vulnerable delegation of dns resolution," in *European Symposium on Research in Computer Security*. Springer, 2013, pp. 219–236.

[6] X. Zheng, C. Lu, J. Peng, Q. Yang, D. Zhou, B. Liu, K. Man, S. Hao, H. Duan, and Z. Qian, "Poison over troubled forwarders: A cache poisoning attack targeting DNS forwarding devices," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 577–593.

[7] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security CCS*. ACM, 2020.

[8] K. Man, X. Zhou, and Z. Qian, "Dns cache poisoning attack: Resurrections with side channels," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 3400–3414.