Poster: X-Ray Your DNS

Amit Klein[§], Vladimir Kravtsov[§‡], Alon Perlmuter[§‡], Haya Shulman[§‡] and Michael Waidner[§‡]
§Fraunhofer Institute for Secure Information Technology SIT
‡The Hebrew University of Jerusalem

ABSTRACT

We design and develop DNS X-Ray which performs analyses of DNS platforms on the networks where it is invoked. The analysis identifies the caches and the IP addresses used by the DNS platform, fingerprints the DNS software on the caches, and evaluates vulnerabilities allowing injection of spoofed records into the caches. DNS X-Ray is the first tool to perform an extensive analysis of the caching component on the DNS platforms.

In addition, DNS X-Ray also provides statistics from previous invocations, enabling networks to check which for popular DNS software on the caches, the number of caches typically used on DNS platforms and more.

We set up DNS X-Ray online, it can be accessed via a website dns.xray.sit.fraunhofer.de.

1 INTRODUCTION

Domain Name System (DNS), [RFC1034, RFC1035], was conceived in the 80s as a basic lookup functionality. Since then DNS evolved into a complex ecosystem. It is increasingly utilised to facilitate a wide range of applications and constitutes an important building block in the design of scalable network architectures. Nowadays DNS resolution platforms are typically composed of multiple IP addresses and caches, which may be hosted on different networks and operated by different entities. The configuration, software and location of these components has direct impact on the security and performance of networks. In practice, network operators often have only a vague knowledge of the configuration of their DNS platforms, on the devices that are connected, the number of caches used, the operating systems (OSes) and DNS software (SW) that they are running, in which networks and Internet Service Providers (ISPs) the resolving machines are hosted, and more. Understanding the inner workings of DNS is important also for design of defences for DNS and mechanisms that utilise DNS, e.g., client subnet in DNS queries [RFC7871].

Measuring DNS Platforms. Due to the significance of DNS and its increasing complexity, the research and operational communities invest considerable efforts to study the DNS infrastructure; see Related Work, Section 2. [9] measured the client side of the DNS infrastructure of *open* resolvers, in order to identify the hosts that communicate with the clients and nameservers in DNS lookups. Recently [6] studied vulnerabilities in caches to injection of spoofed records. [5] devised approaches for measuring the internal components of DNS infrastructure. We build upon the methodologies for studying the DNS platforms presented in [5] to design and implement a tool we call DNS X-Ray for evaluation of DNS resolution platforms. We create a webpage through which DNS X-Ray can be accessed and invoked dns.xray.sit.fraunhofer.de, and upon invocation it analyses the DNS platform on the network on which it is run. During the analysis, DNS X-Ray identifies different components on the platform and discovers and characterises the DNS caches, including the DNS software on the caches, and the vulnerabilities in the caches that allow injection of DNS records.

DNS X-Ray also provides statistics of all the DNS platforms on which it was evaluated. Therefore, clients obtain information not only about the DNS platforms on their networks but can also compare the results to the other platforms in the Internet.

The challenge with studying the caches is that the caches cannot be directly accessed neither by the clients nor by the nameservers, and all the communication with the caches is performed via the ingress and egress resolvers on DNS platforms (see Figure 1). In addition, there are also intermediate caches, such as those in the operating systems or in browsers, we also explain how DNS X-Ray bypasses the intermediate caches.

DNS X-Ray also identifies all the IP addresses used by the tested DNS platform, which networks and ISPs host the DNS platform, and also checks for adoption of best security practices, see [RFC5452], such as whether the ports' and transaction identifiers (TXIDs) are securely selected, and if the caches are vulnerable to injection of spoofed records. This enables security experts as well as non experts to learn about the misconfigurations or vulnerabilities on their networks and allows network and security researchers to obtain insights into DNS resolution platforms in different networks and countries. We make the DNS X-Ray tool as well as the statistics available at `use dns.xray.sit.fraunhofer.de`. Furthermore, DNS X-Ray tool is the first to enable an in depth study of the caching component on DNS platforms. It improves the current understanding of the DNS resolution platforms and serves as a building block for further research on DNS performance and security.

DNS Resolution Platforms. DNS X-Ray studies complex as well as simple DNS platforms; a general model for DNS resolution platforms is illustrated in Figure 1. The platform consists of a set (2^{32-x}) of ingress IP addresses which handle DNS queries from the clients, a set of n caches, and a set (2^{32-y}) of egress IP addresses, which communicate with the nameservers if the queries from the clients cannot be satisfied from (one of) the caches.

This infrastructure corresponds to complex platforms such as Google Public DNS, and it can also be abstracted to incorporate a very simple version for a DNS resolution platforms with a single IP

CCS '17, October 30-November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3138821

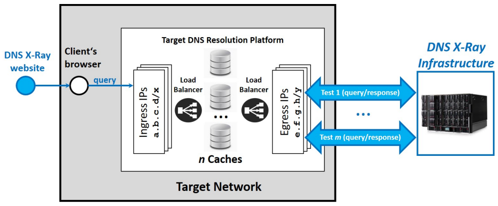

Figure 1: DNS X-Ray and DNS platforms.

address which performs both the ingress and egress functionalities and uses a single cache.

2 RELATED WORK

Recently, Schomp et al [9], measured the client side of the DNS infrastructure of *open recursive resolvers*, in order to identify the different hosts that participate in DNS lookups. Their study focused only on IP addresses that communicate either with the name servers or the clients and does not go deeper into the caching components and the mapping between the IP addresses and the caches. DNS X-Ray provides insights into the caching component and its interaction with the other components in DNS platforms.

A number of other studies were conducted on open resolvers, e.g., [7, 10], where the IPv4 address block is scanned for hosts responding to requests on port 53. However, recently it was shown by [2, 15] that most such open resolvers are either (misconfigured) home routers and mismanaged (security oblivious) networks or malicious networks operated by attackers (where the open DNS resolver is set up for malware communication to the command and control servers). Our study focuses on studying the internal structures of DNS platform, fingerprinting the software of DNS caches, evaluating vulnerabilities to cache injection (by overwriting cached records with new values), and other properties of DNS resolvers.

To optimise content distribution networks (CDNs) [11] ran a study associating DNS resolvers with their clients, and also designed approaches to fingerprint the DNS software passively (on DNS traces). Their study was performed on a limited set of DNS software (Bind9, Mac OS X and Microsoft) using `nslookup` and tracing the queries' pattern issued by the resolver in the lab. This work was extended by [1], which fingerprinted a limited set of DNS software (Bind, Unbound and Microsoft) but also without using active fingerprinting methods in the wild. Both works [1, 11] use flags and fields in DNS header (incl. `CD, DO`, to EDNS and CNAME chains), and patterns in DNS queries to fingerprint DNS software; example patterns include the maximal queried length of `CNAME` chains, presence of requests for `AAAA` (following requests for `A` records). Turning DNSSEC (DO bit in EDNS) and IPv6 off would prevent them from distinguishing between different resolvers' software.

Prior work, [14], also used server selection mechanism to perform an in lab fingerprint of resolver software of DNS software, Bind, PowerDNS, Unbound, DNSCache, MicrosoftDNS. The nameserver selection allows to characterise the software used by the egress DNS resolver. Server selection behaviour can be modified in the configuration file by adjusting the `target-fetch-policy` to 0 0 0 0 0 in Unbound. This will cause the resolver not to fetch additional nameservers and to use only one.

In contrast to previously proposed approaches DNS X-Ray allows repetitive and evaluation of networks, identifies a wide range of DNS software, and can detect vulnerabilities in caches it has not modelled before.

A study by [8] suggested to remove the DNS resolution platforms, and to leave the resolution to end hosts, arguing that the overhead on the existing end hosts would not be significant. Our study can be used for analysis of the complexity of the caching component and the impact on the networks if it were removed.

DNS cache poisoning attacks exploit vulnerabilities in caches to inject spoofed records [3, 4, 12].

Also relevant to our research are online tools for measuring the zone configuration in the nameservers and tools for measuring resolvers. AFNIC operates the Zonemaster[1], which crawls domains and provides information about the connectivity and configuration of the zonefile and the nameservers. There are also commercial services, such as[2] which monitor latency and availability of nameservers. Tools for measuring resolvers focus on checking whether the ports are randomly selected. Such service is offered by the DNS OARC via a `porttest` tool. These tools do not provide an insight into the internals of the DNS resolution platforms.

3 DNS X-RAY

System Design. DNS X-Ray is composed of a client side script running in browsers, nameservers hosting our zone files to which we trigger DNS requests and a website, which displays the analysis of DNS platforms and statistics in form of graphs and charts of all the collected data. DNS X-Ray components are illustrated in blue in Figure 1. Using our own nameservers allows us to receive requests from the tested DNS platforms and based on requests/responses to learn information about the components in a tested DNS platform. We use two hierarchies in DNS for our study each is configured in a separate zonefile. DNS X-Ray is running on four Ubuntu servers and uses MongoDB to store the collected raw data. Our implementation of the DNS resolution functionality is based on the Stanford DNS server. The analysis of the statistics is performed by Perl scripts on the webserver.

Methodology. DNS X-Ray uses the standard DNS request/response behaviour. Client side script triggers specially crafted DNS requests for records in our domains. The DNS requests (including the requested records and their type), that arrive from the DNS platforms at our nameservers, are used to infer information about the caches hidden behind the IP addresses of the tested DNS platform. DNS X-Ray 'decouples' the caches from the IP addresses and counts the number of caches and the IP addresses. Based on the caching behaviour, specifically *eviction of cached records* and *overwriting of the cached records with new values*, we learn the DNS software on the caches. DNS X-Ray also infers the operating system on the caches based on ports' allocation by egress IP addresses in DNS platform.

Data Collection and Statistics Generation. After each evaluation of DNS X-Ray on a new network the data is added to the

[1] `http://zonemaster.net/`

[2] `http://dnscheck.pingdom.com/`

database and the statistics are recalculated to incorporate the new results.

We analyse the collected data and generate the following output: the number of caches used by the tested DNS resolution platform, DNS software on the caches, number of egress IP addresses, networks and countries where the egress IP addresses are hosted, whether the egress resolvers use random source ports and TXIDs.

The focus of DNS X-Ray is to collect the basic information about the components on the DNS platforms, and in particular to characterise the caching component, e.g., its software. Nevertheless, we implemented DNS X-Ray in a modular way so that we can easily extend it with new graphs and charts. Specifically, we store *all* the collected data during the evaluation of a given DNS platform in a database, hence we can define new graphs that would be calculated over all the previously collected data. For instance, we can extend DNS X-Ray to present statistics about the latency to each DNS platform, nameserver selection, IP identifier assignment or even support of cryptography, such as DNSSEC validation [RFC4033-RFC4035].

Non-Exposure to Attacks. DNS X-Ray does not expose to attacks neither the network on which it is evaluated nor other networks. A user can only evaluate the security of DNS platform on a network to which it has access. This does not introduce an additional threat to the network on which a user evaluates DNS X-Ray. Since the user anyway has access to its network - it can itself trigger queries to DNS platform to evaluate its security. We do not allow evaluating networks to which a user does not have access to. Finally, the traffic volume that is generated to measure the DNS platform is moderate (14 tests each repeated 30 times) and lasts for 5-10 minutes.

Bypassing Local Caches. Upon invocation on a given network, a script running in client's browser causes the stub resolver on client's machine to send DNS requests to the resolution platform (Figure 1). However, since DNS X-Ray does not have a direct access to the DNS resolution platform, the requests will go through intermediate caches; see [5] for more details. To cope with intermediate caches DNS X-Ray maps the same hostname to multiple aliases using CNAME records. We setup q DNS records in our `cache.example` zone mapping them to CNAME DNS record as follows:

```
x-1.cache.example   IN CNAME name.cache.example
x-2.cache.example   IN CNAME name.cache.example
...
x-q.cache.example   IN CNAME name.cache.example
name.cache.example  IN A     a.b.c.d
```

Then the script running in client's browser triggers q DNS requests for names `x-1.cache.example`,...,`x-q.cache.example`. The local caches are not involved in the resolution process (specifically in resolving the CNAME redirection) and only receive the final answer.

4 CONCLUSIONS

Our current view of basic Internet components is based on standardisation documents and initial designs. However, most systems significantly evolved since their conception. Furthermore, typically the networks or Internet operators make different choices when setting up their infrastructure. In order to evaluate or improve security of the basic Internet components a clear understanding thereof is important. We design and implement DNS X-Ray - which enables users to evaluate DNS platforms and security of their components, as well as to obtain collective information about DNS platforms in other networks in the Internet. DNS X-Ray is important to allow clients to identify vulnerabilities in their DNS platforms even if DNSSEC validation [RFC4033-RFC4045] is applied. This ensures security even when DNSSEC is incorrectly adopted [13].

ACKNOWLEDGEMENT

The research reported in this paper has been supported in part by the German Federal Ministry of Education and Research (BMBF), by the Hessian Ministry of Science and the Arts within CRISP (www.crisp-da.de/) and co-funded by the DFG as part of project S3 within the CRC 1119 CROSSING. This work was also partially supported by the HUJI Cyber Security Research Center in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office.

REFERENCES

[1] Ruetee Chitpranee and Kensuke Fukuda. 2013. Towards passive DNS software fingerprinting. In *Proceedings of the 9th Asian Internet Engineering Conference*. ACM, 9–16.

[2] David Dagon, Niels Provos, Christopher P Lee, and Wenke Lee. 2008. Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority.. In *NDSS*.

[3] Amir Herzberg and Haya Shulman. 2013. Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org. In *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 224–232.

[4] Amir Herzberg and Haya Shulman. 2013. Socket overloading for fun and cache-poisoning. In *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 189–198.

[5] Amit Klein, Haya Shulman, and Michael Waidner. 2017. Counting in the Dark: Caches Discovery and Enumeration in the Internet. In *The 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*.

[6] Amit Klein, Haya Shulman, and Michael Waidner. 2017. Internet-Wide Study of DNS Cache Injections. In *INFOCOM*.

[7] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. 2015. Going wild: Large-scale classification of open DNS resolvers. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*. ACM, 355–368.

[8] Kyle Schomp, Mark Allman, and Michael Rabinovich. 2014. DNS resolvers considered harmful. In *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*. ACM, 16.

[9] Kyle Schomp, Tom Callahan, Michael Rabinovich, and Mark Allman. 2013. On measuring the client-side DNS infrastructure. In *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 77–90.

[10] Kyle Schomp, Tom Callahan, Michael Rabinovich, and Mark Allman. 2014. Assessing dns vulnerability to record injection. In *Passive and Active Measurement*. Springer, 214–223.

[11] Craig A Shue and Andrew J Kalafut. 2013. Resolvers revealed: Characterizing DNS resolvers and their clients. *ACM Transactions on Internet Technology (TOIT)* 12, 4 (2013), 14.

[12] Haya Shulman and Michael Waidner. 2014. Fragmentation considered leaking: port inference for DNS poisoning. In *International Conference on Applied Cryptography and Network Security*. Springer, 531–548.

[13] Haya Shulman and Michael Waidner. 2017. One Key to Sign Them All Considered Vulnerable: Evaluation of DNSSEC in Signed Domains. In *The 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*. USENIX.

[14] Yingdi Yu, Duane Wessels, Matt Larson, and Lixia Zhang. 2012. Authority Server Selection of DNS Caching Resolvers. *ACM SIGCOMM Computer Communication Reviews* (April 2012).

[15] Jing Zhang, Zakir Durumeric, Michael Bailey, Mingyan Liu, and Manish Karir. 2014. On the Mismanagement and Maliciousness of Networks. In *to appear) Proceedings of the 21st Annual Network & Distributed System Security Symposium (NDSS'14), San Diego, California, USA.*