A Brief Review of DNS, Root Servers, Vulnerabilities and Decentralization

Mallory Runyan
Old Dominion University

COVA CCI Paper 7 Dec 2022

Mallory Runyan

Old Dominion University

A Brief Review of DNS, Root Servers, Vulnerabilities and Decentralization

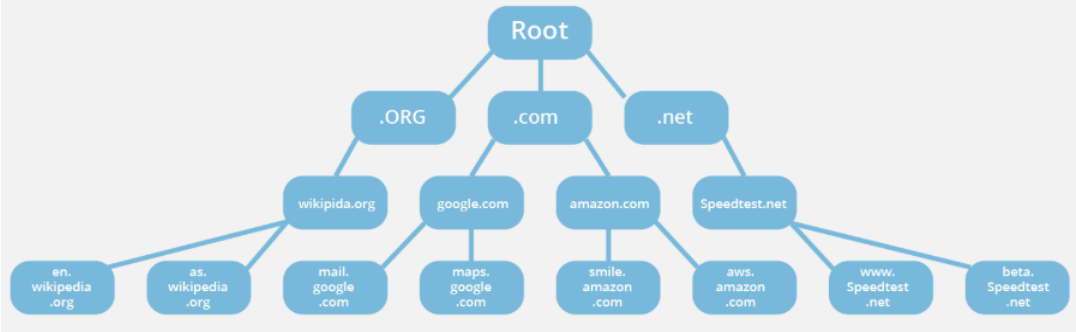
1. Introduction

Since the 1980's and creation of the World Wide Web, Internet utilization is a common and arguably, necessary, part of daily life. The internet is young and still relatively new, but as of 2016, 3.4 billion people were online, and that number has since grown [1]. This is a significant number, but as such a common part of daily life, how elements of the internet or its infrastructure work is complex. The world would very likely be thrown into dark ages if DNS or any other significant aspect of the internet's infrastructure were to succumb to an attack. The Colonial Pipeline ransomware attack in 2021, is a small example of the impacts that cyberattacks can and do have on our daily lives. The research presented is an effort to educate and review current workings of the DNS, its structure and vulnerabilities, and explore new research ideas that better protect and defend the DNS. As it is entangled with many elements of critical infrastructure, it is necessary to continue to educate and survey what we know about the inner workings of the internet. This paper intends to give a brief, yet moderate description of a few of these elements, such as; DNS structure, Root Servers, vulnerabilities, and proposed methods for increasing the security of critical components and infrastructure of the internet.

2. A Brief Review of DNS, Root Servers, Vulnerabilities and Decentralization

2.1 DNS

DNS stands for "Domain Name System" and is often described as the internets' phonebook. Anytime a user accesses information on the internet through a domain name, simply the typed text we know as amazon.com or google.com or any other of the 300 million or so registered domain names [2], that domain name maps to an Internet Protocol or IP address. DNS translates the Domain names or hostnames to IP addresses [2]; this is accomplished via the DNS hierarchy, which loosely resembles the structure of a tree, where a user's initial domain request moves through zones that do not overlap [3]. The basic structure is an inverted tree, with the Roots or Root Servers at the top. Top Level Domains (TLD's) such as .com or.edu are just below the Root Servers, with second and third level domains such as google and apple (second) world wide web (www) or mail as third level domains [4]. Depending on the chart or illustration, "host" may make up the bottom of the inverted tree. In this paper, the focus will primarily be on DNS and Root Servers or Root Zone (used interchangeably).



Example DNS hierarchy sourced from https://www.cloudflare.com/learning/dns/glossary/dns-root-server/

2.2 Root Server

DNS Root Servers or simply “Root Servers” are an integral part of the DNS hierarchy. Although there are many root servers, there are only 13 Root IP addresses used to query the many root server networks, containing 1585 instances as of this writing, operated by 12 independent organizations [4] [5]. However, each organization cooperates with the 11 other Root Server Organization or “Operators”; the 13 IP addresses using “Anycast” routing, which allows groups of servers over a geographic area to share an IP address and “is a technique used to share the load of a variety of global services” [6][7].

Verisign, INC operates two of the 13 root servers, a.root-server.net or A-root and j.root-servers.net or J-root, with IPv4 and IPv6 addresses 198.41.0.4/2001:503:ba3e::2:30 for A-root and 192.58.128.30, 2001:503:c27::2:30 for J-root [5][8][17].

Second on the list is the University of Southern California Networking and Cybersecurity Division which operates b.root.servers.net or B-root server, with IPv4 and IPv6 addresses 199.9.14.201 and 2001:500:200::b [5] [9]. The third server is c.root-servers.net or C-root and its operated by Cogent Communications, with IPv4 and IPv6 addresses 192.33.4.12 and 2001:500:2::c [5] [10]. D.root-servers.net or D-root, is operated by the University of Maryland, with IPv4 and IPv6 addresses 199.7.91.13 and 2001:500:2d::d [5] [11].

NASA operates the fifth server, e.root-servers.net or E-root, with IPv4 and IPv6 addresses 192.203.230.10 and 2001:500:a8::e [1] [12]. Specifically, the Information Technology Operations Division at NASA Ames Research Center operates E-Root, operating 308 server sites across the globe [5] [12]. Sixth on the list is the f.root-servers.net or F-root, which is operated by Internet Systems Consortium. F-root addresses are 192.5.5.241 and 2001:500:2f::f [5] [13].

DISA DOD Network Information Center is one of the 12 organizations and operates g.root-servers.net or G-root, with IPv4 and IPv6 addresses 192.112.36.4 and 2001:500:12::d0d [1] [14]. The U.S. Army Research Laboratory operates h.root-servers.net or H-root, with IPv4 and IPv6 addresses 198.97.190.53 and 2001:500:1::53 [5] [15].

The ninth root server, i.root-servers.net or I-root, is operated by Netnod, and according to their site, they were the first root server to be located outside of the United States. I-root addresses are 192.36.148.17 and 2001:7fe::53 [5] [16]. The Ripe Network Coordination Centre operates the eleventh server, k.root-servers.net or K-root, with IPv4 and IPv6 addresses 193.0.14.129 and 2001:7fd::1 [5] [18]. L.root-servers.net or L-root, is operated by ICANN, the Internet Corporation for Assigned Names and Numbers, with IPv4 and IPv6 addresses 199.7.83.42 and 2001:500:9f::42 [5] [19]. The WIDE Project operates the last root server, m.root-servers.net or M-root, with IPv4 and IPv6 addresses 202.12.27.33 and 2001:dc3::35 [5][20].

In total, the United States operates 10 of the 13 Root Servers, 3 of which are operated by the US Government or military agencies and the remaining 7 operated by US based organizations [3]. The last 3 Root Servers are based in Japan, Sweden, and the Netherlands [3].

2.3 Vulnerabilities of DNS and Root Servers

The IEEE conference paper *Survey on Domain Name System Security* [21] categorizes weaknesses of DNS into five separate groups, 2 of which will be expanded: cache poisoning, where an attacker tries to spoof a recursive DNS server [22]. Here, “Recursive” is referring to a Recursive DNS resolver, which provides the IP address the “client” or user requests [22].

A cache poisoning attack happens when a user types in the domain or URL, correctly, into a web browser and the recursive DNS server under the attacker's control returns the user a compromised or malicious IP address [21]. “Unrelated Data attack” and “Related Data Attack” are two types of cache poisoning attacks. In an Unrelated Data attack, “the attacker controls a malicious

authorization server, and inserts unrelated resource records in answer area when the recursive server requests resource records of the domain, attempting to make the recursive server accept these faked data together." [21] Through a Name-server record (NS), a "Related Data Attack will connect victims' domain names with [the] attackers…..then forge a record for the domain name of the victim." [21]

The second group is a denial-of-service attack, or DOS, which is as it sounds, denying access to service. This type of attack attempts to make parts of the internet inaccessible or "paralyzed", or maybe just a website inaccessible, by spamming or flooding the DNS with requests until the server breaks down [21] [23]. One type of DOS attack is known as "flash-crowd" attack [23], wherein compromised hosts, upwards in the millions, generate queries that overwhelm the DNS. This attack is difficult to mitigate because legitimate clients are continuing to generate queries as well, and filtering between these poses a challenge [23]. Because of its importance and vulnerabilities, DNS is a highly targeted, "main objective of internet attacks." [21]; As Root Servers have fixed IP addresses "that cannot be easily modified", they are therefore not as easily protected by traditional defenses [23].

2.4 Decentralization

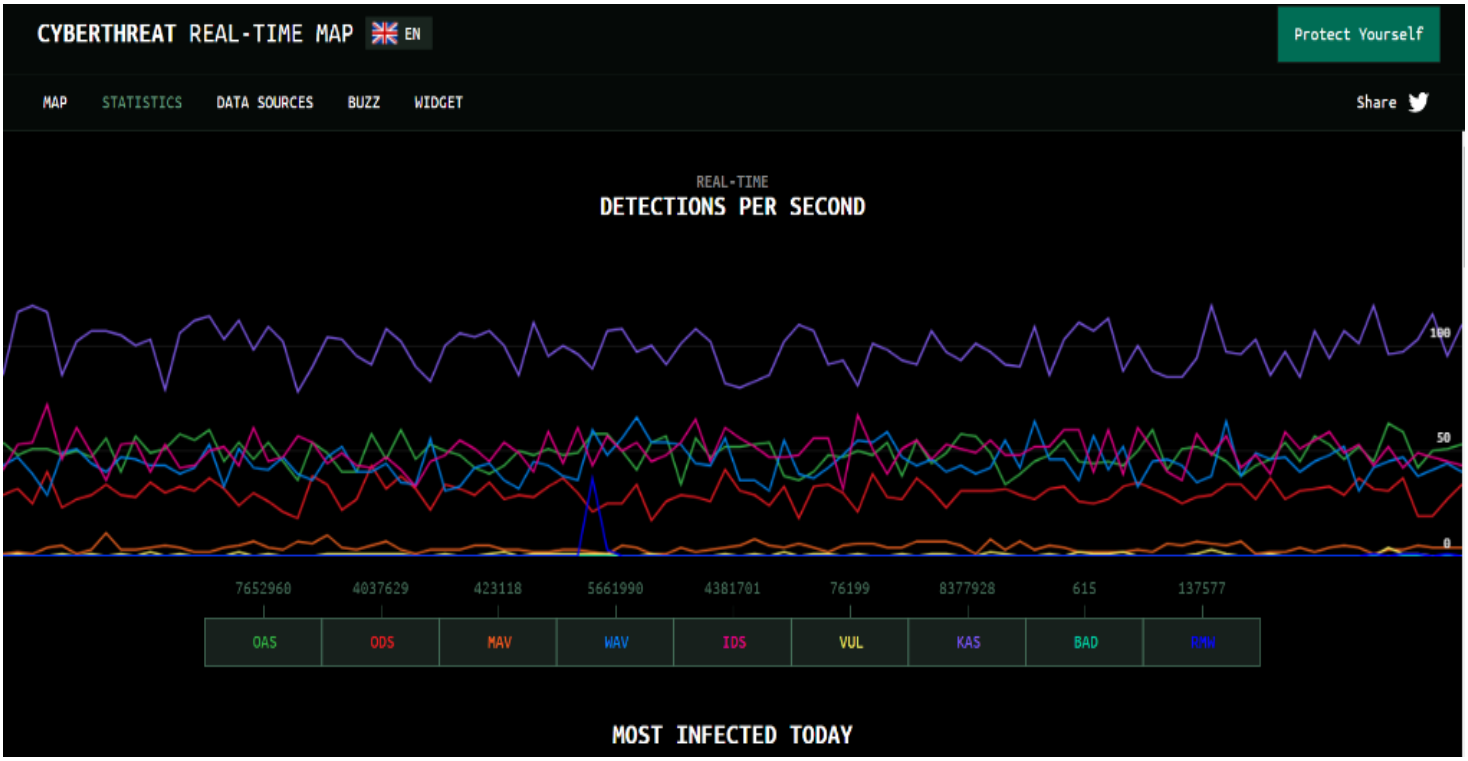
The importance of DNS and Root Servers cannot be overstated. The following briefly explores two methods to decentralize root zone management, remove the trust dependency and decrease risk to the DNS by mitigating the current system setup that is a single point of failure (SPOF) [24] [25].

Blockchain literature [24] proposes decentralization and improved operation transparency via RootChain, with four goals: Uniform Global Namespace, Anti-SPOF risk, Transparency and Accountability, and lastly, Compatibility. [24] Current identified problems and arguments for the utilization of RootChain, which is a Blockchain system, are the SPOF risk and lack of transparency and accountability in root zone management. The SPOF risk is based on the bottleneck of the IANA (Internet Assigned Numbers Authority) function operator, in that "all submitted data need to be aggregated to the role of IANA function before it can be written to the root zone database…"[24]. The lack of transparency and accountability stems from the private nature of details relating to root zone management, and root zone maintainers unable to view change records of the zone management or administrator approval process [24]. The proposed implementation of RootChain would be an effort to separate "..TLD data publication from TLD delegation…", distribute the root zone operation while maintaining single root authority, and authenticating and publishing Root Zone Data "by delegated TLD authorities directly into the ledger of RootChain." [24]. Smart contracts designed for the life cycle of TLD would improve upon transparency and accountability with the literature [24] proposing that RootChain is a "first step towards distributed root zone operation in DNS". [24]

The second method is DNS without Root Servers [25]. As stated previously, the DNS hierarchical structure is tree shaped; DNS architecture consists of resolvers and name servers, and introduced into this system is DNSSEC, which stands for DNS Security Extensions and is public-key cryptography [25]. Zone administrators have a private key that signs Domain name records and after the authentication of the public key, resolvers then verify the signature and "authenticate zone keys by following the chain of keys up to the root, which is signed by a key known to the resolver." [25] The proposed decentralization of this method is to skip the root; the resolver would hold the same information as the root, TLD's, authoritative name servers, IP addresses and the public-key [25]. Removing or "cutting off the root" allows for the "authority of a TLD operator [to be] limited to their own namespace, whereas the authority of root includes all TLDs." [25] This proposed method is still hierarchical and still requires trust, but "eliminate[s] a single point of trust." [25]

3. Conclusion

As with the internet, security and protections of its infrastructure is still a young and relatively new process. Sites such as https://cybermap.kaspersky.com/, track cyber threats and attacks, with the number of attacks reaching into the millions daily [26]. The screengrab below is a snapshot taken of real-time detection from multiple scanners on https://cybermap.kaspersky.com/stats,



which resets everyday at 00:00 GMT. The colored lines represent the different scanners or “detection flow”. For example, OAS, which stands for On-Access Scan and is the bright green graph line, and “shows malware detection flow during On-Access Scan, i.e. when objects are accessed during open, copy, run or save operations.” KAS, which is the purple graph line and stands for Kaspersky Anti-Spam, has the highest detections per second at 8,377,928 detections at the time this was taken[26]. Numbers like this can seem overwhelming, but just as attacks evolve and become more sophisticated, the same is true for greater protection of data, such as encryption or multi-factor authentication (MFA), as well as defenses and even counter-attacks against bad actors. From the birth of the internet and subsequent explosion of connectivity, bad actors will continue to attack and exploit countries, corporations, critical infrastructure, and individuals alike. It is important to continue researching and exploring new and better ways of protecting the internet and shoring up its critical infrastructure.

References

1. M. Roser, H. Ritchie, and E. Ortiz-Ospina, “Internet,” *Our World in Data*, 14-Jul-2015. [Online]. Available: https://ourworldindata.org/internet. [Accessed: 07-Dec-2022].
2. “What is a domain name? | domain name vs. URL | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/. [Accessed: 07-Dec-2022]. (28)
3. M. Wander, C. Boelmann, and T. Weis, “Domain Name System without root servers,” *Lecture Notes in Computer Science*, pp. 203–216, Jan. 2018.
4. “DNS root server | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/dns-root-server/. [Accessed: 07-Dec-2022].
5. *Root Servers*. [Online]. Available: https://www.iana.org/domains/root/servers. [Accessed: 07-Dec-2022].
6. O. Bonaventure, “The January 2018 issue,” *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 1, pp. 1–2, 2018.
7. D. Cicalese, D. Giordano, A. Finamore, M. Mellia, M. Munafò, D. Rossi, and D. Joumblatt, “A First Look at Anycast CDN Traffic,” *arXiv.org*, 12-Mar-2021. [Online]. Available: https://doi.org/10.48550/arXiv.1505.00946. [Accessed: 07-Dec-2022].
8. “How Verisign Operates Internet Root Servers – Verisign,” *How Verisign Operates Internet Root Servers – Verisign*. [Online]. Available: https://a.root-servers.org/. [Accessed: 07-Dec-2022].
9. “B root,” *B Root*. [Online]. Available: https://b.root-servers.org/. [Accessed: 07-Dec-2022].
10. “Root homepage,” *C*. [Online]. Available: https://c.root-servers.org/. [Accessed: 07-Dec-2022].
11. “Root Home Page,” *D*. [Online]. Available: http://d.root-servers.org/. [Accessed: 07-Dec-2022].
12. A. R. C. W. Group, “Ames Research Center,” *E.root*. [Online]. Available: https://e.root-servers.org/. [Accessed: 07-Dec-2022].
13. I. S. Consortium, “F-root,” *ISC*, 10-Jul-2019. [Online]. Available: https://www.isc.org/f-root/. [Accessed: 07-Dec-2022].
14. “G-Root,” *DISA*. [Online]. Available: https://disa.mil/g-root. [Accessed: 07-Dec-2022].
15. “H-Root will change its addresses on 1 December 2015,” *H.ROOT*. [Online]. Available: https://h.root-servers.org/renumber.html. [Accessed: 07-Dec-2022].
16. “Operational statement for i.root-servers.net,” *Netnod*. [Online]. Available: https://www.netnod.se/i-root/operational-statement-for-i.root-servers.net. [Accessed: 07-Dec-2022].
17. “How verisign operates internet root servers – verisign,” *How Verisign Operates Internet Root Servers – Verisign*. [Online]. Available: http://j.root-servers.org/. [Accessed: 07-Dec-2022].
18. Created: 16 Feb 2018 - Last updated: 28 Mar 2022, “K-root,” *RIPE Network Coordination Centre*. [Online]. Available: https://www.ripe.net/analyse/dns/k-root. [Accessed: 07-Dec-2022].
19. “ICANN managed Root Server,” *Go to ICANN DNS Engineering*. [Online]. Available: https://www.dns.icann.org/imrs/. [Accessed: 07-Dec-2022].
20. “Root DNS server,” *M*. [Online]. Available: https://m.root-servers.org/. [Accessed: 07-Dec-2022].
21. F. Zou, S. Zhang, B. Pei, L. Pan, L. Li, and J. Li, “Survey on domain name system security,” *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, 2016.

22. H. Berger, A. Z. Dvir, and M. Geva, “A wrinkle in time: A case study in DNS poisoning,” *arXiv.org*, 26-Jun-2019. [Online]. Available: https://arxiv.org/abs/1906.10928v1. [Accessed: 07-Dec-2022].

23. A. S. M. Rizvi, J. Mirkovic, J. Heidemann, W. Hardaker, and R. Story, “Defending Root DNS Servers Against DDoS Using Layered Defenses,” *arXiv.org*, 15-Sep-2022. [Online]. Available: https://arxiv.org/abs/2209.07491. [Accessed: 07-Dec-2022].

24. Y. Zhang, W. Liu, Z. Xia, Z. Wang, L. Liu, W. Zhang, H. Zhang, and B. Fang, “Blockchain-Based DNS Root Zone Management Decentralization for Internet of Things,” *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–20, 2021.

25. M. Wander, C. Boelmann, and T. Weis, “Domain Name System without root servers,” *Lecture Notes in Computer Science*, pp. 203–216, Jan. 2018.

26. *Kaspersky cyberthreat real-time map*. MAP. (n.d.). Retrieved December 7, 2022, from https://cybermap.kaspersky.com/

27. “What are root name servers?,” *Netnod*. [Online]. Available: https://www.netnod.se/i-root/what-are-root-name-servers#:~:text=Root%20name%20servers%20are%20the,%3A1%3A3%3A%3A67. [Accessed: 07-Dec-2022].

28. “What is a Root Server?,” *netnod.se*, 13-Feb-2014. [Online]. Available: https://www.netnod.se/sites/default/files/i-root/What_is_a_rootserver_Netnod_fact_sheet.pdf. [Accessed: 07-Dec-2022].

29. S. Jelen, “DNS Root Servers: What Are They and Are There Really Only 13?” [Online]. Available: https://securitytrails.com/blog/dns-root-servers. [Accessed: 07-Dec-2022].

30. “What is DNS? | how DNS works | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-dns/. [Accessed: 07-Dec-2022].