Laura M Saxton
LCYS_2022
CDF 2

Summary Post

1. DNS Cache Poisoning

DNS cache poisoning is a spoofing attack where an actor intercepts package requests sent to the IP address of a target domain and reroutes user traffic to a malicious site . Such attacks can happen at both the resolver and client-side levels (Abu-Ghazaleh et al., 2019), and can be prevented through use of the DNSSEC extension and a Virtual Private Network (VPN), respectively.

2. DNSSEC Extensions

DNSSEC extensions provide “end-to-end protection through the use of digital signatures” (Stallings, 2016: 641). These signatures safeguard domain address requests sent to a DNS against unverified websites attempting to reroute user traffic.

While the DNSSEC extension is protocol standard, “it does *not* provide privacy protections for lookups” (Cloud, n.d.), leaving some clients vulnerable. Additionally, Shor’s algorithm, used by quantum computers to break current public-key cryptography (de Jong et al., 2020; Hines, 2022), could render this extension obsolete.

One solution could be implementing DNSSEC with DNS-over-TLS (DoT) (Teh, 2022), which “protects the privacy of DNS queries and prevents man-in-the-middle attacks against DNS responses” (Nakatsuka et al., 2019). DoT can be used with encrypted DNS, which could protect public-keys (de Jong et al, 2020). While DoT is comprehensive, it “requires more resources at recursive resolvers and name servers” (de Jong et al., 54) and needs more research to assess these variables.

3. Virtual Private Networks

A Virtual Private Network (VPN) seems a sound method for preventing client-side attacks, as VPNs establish “a secure and encrypted tunnel to transfer data” (Sun et al., 2021: 1). VPNs can be proprietary or open-source and thwart an attacker’s ability to target the IP address of a single user.

Yet this solution may be prohibitive for those who find VPNs cumbersome for everyday use. Establishing an automatic connection through a gateway VPN upon login (Bohus, 2022; SocialBizWire, 2019) could circumvent this issue, but large-scale implementation would require careful consideration by networking companies.

4. Conclusion

Though DNS cache poisoning is a common attack, there are protection mechanisms at the client-side and resolver levels. Individuals can use VPNs to mask their IP addresses, while networks can use the DNSSEC protocol to secure DNS responses. There are strengths and weaknesses to both methods.

Resources

Abu-Ghazaleh, N., Alharbi, F., Chang, J., Qian, F., Qian, Z. and Zhou, Y., 2019. Collaborative Client-Side DNS Cache Poisoning Attack. In: *IEEE Conference on Computer Communications 2019*. [online] IEEE. Available at: https://ieeexplore.ieee.org/document/8737514 [Accessed 18 July 2022].

Ballmann, B., 2021. *Understanding Network Hacks*. 2nd ed. SPRINGER.

Borhus, T., 2022. Peer Response – Thomas Borhus. [Blog] *Re: Initial Post -- Laura Saxton*, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=114698 [Accessed 7 August 2022].

de Jong, J., Müller, M., Overeinder, B., van Heesch, M., and van Rijswijk-Deij, R., 2020. Retrofitting post-quantum cryptography in internet protocols. *ACM SIGCOMM Computer Communication Review*, 50(4), pp.49-57.

Hines, J., 2022. Peer Response – James Hines. [Blog] *Re: Initial Post -- Laura Saxton*, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=114698 [Accessed 7 August 2022].

Google Cloud. n.d. *DNS Security Extensions (DNSSEC) overview | Google Cloud*. [online] Available at: https://cloud.google.com/dns/docs/dnssec [Accessed 18 July 2022].

Lazarevski, B., n.d. O*WASP: Anatomy of a DNS Cache Poisoning Attack*.

Nakatsuka, Y., Paverd, A. and Tsudik, G., 2019. PDoT: Private DNS-over-TLS with TEE Support. *Digital Threats: Research and Practice*, [online] 2(1), pp.1-22. Available at: https://arxiv.org/pdf/1909.11601.pdf.

Stallings, W., 2016. *Cryptography and Network Security*. Harlow: Pearson Education, Limited.

SocialBizWire, 2019. Ethernity Networks introduces programmable VPN gateway. [online] Available at: <https://advance.lexis.com/document/?pdmfid=1519360&crid=008da904-4eb4-43ef-9f6f-9b02067f0d42&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5VHD-YDW1-F0K1-N53Y-00000-00&pdcontentcomponentid=386642&pdteaserkey=sr0&pditab=allpods&ecomp=rbzyk&earg=sr0&prid=53c61293-771c-44fb-a3d1-6ccf68fe3076> [Accessed 7 August 2022].

Sun, Y., Wang, B., Wang, C. and Wei, Y., 2021. On Man-in-the-Middle Attack Risks of the VPN Gate Relay System. *Security and Communication Networks*, 2021, pp.1-7.

Teh, X. L., 2022. Peer Response -- Xue Ling Teh. [Blog] *Re: Initial Post -- Laura Saxton*, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=114698 [Accessed 7 August 2022].