Network Security Practices through Anonymity

Prof. Smitha G R, Suprith C Shekar, Ujwal Mirji
Department of Information Science Engineering
R.V College of Engineering
Bengaluru, India smithagr@rvce.edu.in
Department of Mechanical Engineering
R.V College of Engineering
Bengaluru, India suprithcshekar.me18@rvce.edu.in
Department of Mechanical Engineering
R.V College of Engineering
Bengaluru, India ujwalmirji.me18@rvce.edu.in

Abstract
Anonymity online has been an ever so fundamental topic among journalists, experts, cybersecurity professionals, corporate whistleblowers. Highest degree of anonymity online can be obtained by mimicking a normal everyday user of the internet. Without raising any flags of suspicion and perfectly merging with the masses of public users. Online Security is a very diverse topic, with new exploits, malwares, ransomwares, zero-day attacks, breaches occurring every day, staying updated with the latest security measures against them is quite expensive and resource intensive. Network security through anonymity focuses on being unidentifiable by disguising or blending into the public to become invisible to the targeted attacks. By following strict digital discipline, we can avoid all the malicious attacks as a whole. In this paper we have demonstrated a proof of concept and feasibility of securing yourself on a network by being anonymous.

Keywords:
Online privacy, Anonymity, Networks, Virtual Private Networks, Onion Routing, spoofing

1. Introduction

Anonymity corresponds to being unknown, unidentifiable, untraceable and indistinguishable from other users in public domain. Keeping yourself hidden has become simple and a common practice among professionals and experts who don't like being tracked online. Unfortunately, it is a topic that is out of reach for the common public due to their lack of interest as well as knowledge in this subject. The willful ignorance of the general public is a huge benefit to the “Big Tech” companies that capitalize on the information that is made available to them by means of browsing the internet.

Being anonymous online means being able to fully exercise freedom of speech. Online anonymity has made it much easier for people to freely express their views on many topics, some important, some trivial. People struggling with illnesses and life struggles can find support without fear or criticism online, and this is a good thing everyone. Online anonymity offers freedom of movement, allowing users to conduct activities without being judged by others or directly observed by snoopers. With online anonymity, users don’t have to worry too much about their personal safety being compromised as a result of what they can do online. In the enterprise world, employee privacy mitigates the risk of social engineering attacks. The more information an attacker can obtain on the power dynamic within an organization, the easier it is to carry out attacks in a much more targeted and effective manner.

As the number of devices that are going online are increasing by the day through networking advancements like 4G, 5G, Gigabyte internet that are easily accessible by the common public, it is revolutionizing modern society drastically. This gives rise to another concern i.e., online activity surveillance, so it is necessary to generate interest and bring awareness among people to facilitate their understanding of the topic and help them protect their identity and freedom by anonymizing their activities online. Personal data is considered among the most valuable commodities on the internet, and many companies log and analyse user data to conduct business. From consumer behavior to predictive analyses, companies routinely capture, store, and analyze large volumes of quantitative data on their consumer base every day. Some companies have built their entire business model around consumer data, either they sell personal information to a third party or creating targeted ads on the user. So, hackers go out of their way to obtain it. Being anonymous prevents hackers from getting access to sensitive information such personal data, credit card transactions, passwords, and banking information easily. Ergo keeping yourself hidden is the best way to prevent malicious attempts and keep your online security in check.

One of the major drawbacks of online anonymity is it allows the person to do things without having to take responsibility or be associated with it, and thus face no consequences for their activities as a result. Online

Manuscript received April 5, 2024
Manuscript revised April 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.4.18

anonymity can bring an assortment of problems with it. So, we often see it used for criminal objectives like online abuse of the system, illegal activities. Hence it is necessary to bring awareness among people to use Online anonymity in a wise and responsible manner. In development of online security through anonymity we summarize the concept, technology, methods and validate performance and safety of staying anonymous online.

2.Anonymous Networking

Anonymizing yourself through appropriate networking practices is essential in the near future where almost everything is going to be automated/digitized. This paper contains some basic steps to decrease your online presence which can go a long way in safeguarding your privacy as it can increase the time (needed to obtain) or prevent the leak of necessary information that can lead to a targeted attack. Hopefully deterring the would-be attacker who will have to spend extra time and effort in obtaining your data. This however does not make a person completely anonymous as it is not possible to browse the internet without leaving any trace. These methods are intended as a medium to spread information and raise awareness about the need of online security until strict data control laws are implemented.

2.1 Use of Virtual Private Networks:

A Virtual Private Network (VPN) uses secure encryption measures to prevent unauthorized access of data that is being transferred between systems and ensure that data cannot be modified without detection as it flows via the Internet. This creates an encrypted channel (tunnel) across the network to transport the data [1]. In simple terms, it establishes a protected network connection even on public networks. The initial purpose of VPN was to provide access to work servers from any location by creating a private connection which cannot be tampered with.

It is key to look for a trusted provider that has a good reputation in terms of client data storage and logging. So, in this case the consumer has to choose a VPN provider that doesn't log or store any sort of browsing data. VPN can also be used to bypass region locked content as it makes the traffic appear to be originating from the VPN server. The only disadvantage of using a VPN is the slightly slow connection speeds.

2.2 Use of Secure, Virtualized or Temporary OS:

There are many OS’s that are capable of running on minimal resources and run on temporary or virtual instances where the user’s data is not stored in the system permanently and is reset every time the system rebooted. Using such an Operating System for your sensitive work will be the most secure way to avoid surveillance, censorship, advertisements and viruses as the instance of OS is refreshed after every reboot. There are various Operating systems that are capable of running on a USB drive so the setup time for Virtual Machine etc., is avoided and the overall time taken is reduced.

Tails OS is one such operating system made to be portable that protects against surveillance and censorship [2]. It is bootable via a live DVD or live USB and does not leave any digital footprint on the computer unless explicitly told to do so. Tails is by design unable to store data over of different user sessions. It runs solely based on RAM and does not write data to any other drive unless the user decides to do so. All inbound and outbound connections are forced to be made through Tor, and any intrusive connections are blocked. Tails includes a set of tools and software's to work on sensitive documents and communicate secure. Tails OS comes ready-to-use package and is set to most secure settings by default. It also has an optional persistent storage option that encrypts the stored data, so important documents can be stored if the user wants. Tails is free to download, use and is based on Debian GNU/Linux. Independent security researchers can verify it to examine its safety.

Another Operating System specializing in security through isolation is Qubes OS, recommended by Edward Snowden, a former national security agency contractor. Contrary to tails it can be used as a permanent operating system even with all its security features. Qubes OS uses virtualization technology to isolate various programs or applications from each other [3]. It also sandboxes many system components like networking and storage, this way even if one of these programs is vulnerable to attacks it does not affect the integrity of the entire system. It's one of the most effective ways to defend against Zero Day Exploits.

The isolated compartments called Qubes just like the operating systems is categorized by,

i. **Objective:** With a mentioned list of one or many isolated applications, for personal or professional projects, to manage the network stack, the firewall, or other user-defined purposes.

ii. **Ecosystem:** full-fledged or stripped virtual machines are based on popular Distros of Linux, such as Fedora, Debian, and Windows.

iii. **Levels of Credibility:** from absolute to inexistent. All windows are portrayed as a unified desktop ecosystem with unforgeable color-coded window borders so that various security levels are easily identifiable.

Apart from popular Linux distributions like fedora and Debian, Qubes OS can also run windows programs in its virtual machines. This should be a deciding factor for many users to shift from windows to more secure Qubes OS.

2.3 Running traffic through Proxy Chains or TOR circuit

All Network traffic is monitored by your ISPs which is subjected to censorship, inturn controlling user's network activities and actively keep a log of them in their servers. Especially when you are on a public Wi-Fi your browsing history, passwords, and other credentials are easily accessible by the provider. Even if the provider doesnt have any malicious intensions against the user the stored data is vulnerable to Data Breaches which can expose user's data globally that can be easily misused if the user is not aware. It is recommended to route user's network through multiple intermediary machines with random IP addresses that user can control. Proxy Chains is one such tool for this purpose, it forces all TCP connectios made by the given software to go through TOR proxies or SOCKS4, SOCKS5 or HTTP proxies. This allows the user to access the Internet through a restrictive firewall, while hiding their IP address, and bounce network through proxy servers and access their local Intranet remotely via an external proxy. Proxy Chains even enables its users to route though multiple proxies at once by "chaining" them and use programs without any built-in proxy support. Most important reason to use Proxy Chains from a security perspective is to protect the user's identity from being exposed[4].

Connecting to the Internet or the select domain through proxies, the client IP address will be hidden and the IP of the proxy server will be shown in the connection parameters. It provides a client with more privacy than directly connecting to the Internet. Since the traffic is being routed through various nodes located in different places the response time and latency is very high, especially if you use proxies from different countries. This can be solved by using only a few nodes rather than chains to reduce the delays and response times.

In an Onion enabled network, messages or data packets are encoded with layers of encryption, just like the layers of an onion. The encrypted data packets is routed through a series of nodes that form the onion network, after each bounce it "peels" off a layer, reviealing the next destination. When the last layer is decrypted, the message reaches its destination. The sender stays anonymous as only the intermediary node knows only the location of the immediately preceding and subsequet nodes. While routing through an onion network provides a higher level of security and anonymity, there are procedures to break the anonymity of this technique, using timing analysis. If we use VPN to encrypt the traffic, route it into a proxy server and then route it through TOR circuits, user can encrypt all of your traffic to your start point (The VPN Out interface) and send it to the proxy server after which the TOR network would take over. This way you can prevent the VPN provider from knowing that you are accessing a TOR node by routing it through a proxy server first. This is the most common method used by professionals to be anonymous and leave no tracks behind.

2.4 Parody identifiers for Mac Address and IPv4/v6

The media access control address is a distinctive address that is allocated to every device (that is capable of connecting to the internet) as it is manufactured. It is indigenously hard-coded into a computer's network interface card (NIC) and is unique to it [5]. MAC address for an Ethernet adapter is specified in this format 00:0a:95:9d:68:16, It consists of 6 sets of hexadecimal numbers, the first three sets are specific to a manufacturer (so the devices manufactured by the same company will have the first 3 sets same). The remaining 3 sets are unique to the given device. When a specific device is acting suspiciously the administrator can block the network access to thats device by adding the device MAC address to a blacklist. Various advanced approaches are used to detect spoofing and block the devices [6][7].

So if a potential attacker gets access to your mac address, it can be used to gather information and find known vulnerabilities of the manufacturer and will be able to successfully carry out their attack. In order to prevent this from happening, you can use various tools that randomize your mac address and predetermined intervals (every browsing session, every reboot etc.) so the attacker will not have information about the manufacturer of your device and cannot exploit any vulnerabilities.

The IP address is a unique identifier that is designated by the Internet Service Provider (ISP), the 2 types of IP addresses are, v4 and v6. The primary design of the IPv4 did not foresee the growth of the internet and this brought forth the idea to switch the current numbering system of IPv4. The main drawback of IPv4 is the limited availablity of addresses, and to overcome this IPv6 system was developed. Which suppoerted up to **340 trillion trillion trillion IP addresses** whereas IPv4 can support a maximum of **4,294,967,296 IP addresses** [8].

The ISP assigned address can be easily tracked down by using simple online tools with pinpoint accuracy of the general physical location (exact location is some rare cases). So in order to remain secure both physically and online we must prevent sharing our IP address on the internet (which happens by default every time we access it).

2.5 DNS Resolvers and its significance in Network security and performance

The Domain Name System is basically the phonebook of the Internet. It is a server which stores the data of host names mapped to their IP address (can be multiple)[9]. When a domain name is entered in the browser, it first looks up the IP address in the cached memory of the local cached database. If it is not available, it makes a request to the DNS server (by default belonging to your ISP) which resolves the domain name and sends the IP address of the requested site back to your browser. This is cached in the local server for use in the immediate future.

This poses a security risk as the location of the DNS server can be used to determine the general area of your connection, by looking up the DNS request made. There are multiple points where the DNS query can be poisoned (poisoning refers to substituting the real IP address with a fake one and returning it to the computer that requested it)[10].

So the solution to this is, instead of relying on the ISP to resolve the domain and send responses we can start utilizing the DNS services provided by many trustable companies like Cloudflare, Google, OpenDNS that are bound by the International laws governing data security and privacy. They are not only safe but they also remove the middle man(ISP) from tampering with the DNS requests, and maintaining the logs of the requests made by their clients. The advantages of using this service is that the location of the server will not be close to your physical location and the responses cannot be tampered with.

3. Implementation and analysis

This section contains a brief method for implementation of measures that can be taken to safeguard your online privacy. For in depth understanding of these methods, further interest and study is necessary

3.1 Spoofing MAC address

Spoofing MAC address generally requires additional packages to be downloaded on windows, macOS but generally comes pre-installed in Linux distros. Note: In this implementation, we focus on setting up and using the MAC Changer utility on Linux based operating systems. To modify the MAC address the terminal needs to be launched with super user privilege.

To see the permanent MAC address following commands have been used `macchanger -s eth0` for LAN or `macchanger -s wlan0` for Wireless Adapter Information, and make a note of it, this can also be verified by checking the mac address on the connected devices page of the router settings. As an example, once we run the command `macchanger -r eth0` as a root user, the mac address of the ethernet device will be randomized. The process of randomization of MAC address is however not sufficient by itself, therefore various other measures need to be taken in addition to this step [11].

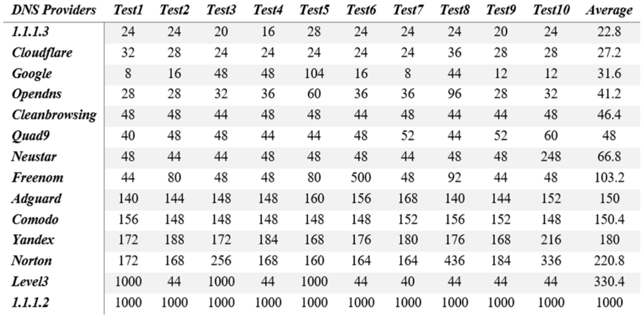
3.2 Identifying and Setting up DNS resolvers for improved performance, safety and Privacy

Changing the DNS settings in Linux is quite effortless, the name server address in the “resolv.conf” file under “etc” folder must be edited. In fact Changing DNS settings for any device these days has become easy. For smartphone devices like Android and IOS the DNS resolver can be changed in the Wi-Fi settings. And for Windows it can be changed in the Network settings. Based on the logic associated with DNS tracing and TCP traffic analysis to understand users perception of performance and universality of failures and errors faced by an user on a network studies have been conducted[12]. There are many companies providing DNS services that support DNS over TLS and HTTPS by default, we performed different performance tests to identify the best DNS provider keeping security and anonymity in mind. We chose the top 7 free DNS providers which are commonly used throughout the world,

- Google 8.8.8.8 , Exclusive and unmonitored access to Internet
- Cloudflare 1.1.1.1 , Exclusive and unmonitored access to Internet
- Quad9 9.9.9.9 , Privatized and security oriented provider, blocking access to malicious websites and domains.
- OpenDNS 208.67.222.222 , Market pioneers first to offer free DNS services and block malicious domains as well as the option to to block adult content.
- CleanBrowsing 185.228.168.168, they are private and security oriented, and blocks access to adult content domains
- Yandex DNS 77.88.8.7: Default filtering of malicious domains. Widely used in Russia.
- Comodo DNS 8.26.56.26, One of the oldest providers in the market, blocking malicious domains by default.

Test was fundamentally simple performing 10 DNS requests to popular and wellknown domains (google, facebook, twitter, gmail, etc) and measured the Round Trip Times (RTT). We averaged all the requests for obtaining an aggregate performance indicator per DNS resolver. For this purpose we used a tool called dnsperftest.

Table 1 RTT test for different DNS Provider in milliseconds



DNS Providers	Test1	Test2	Test3	Test4	Test5	Test6	Test7	Test8	Test9	Test10	Average
1.1.1.3	24	24	20	16	28	24	24	24	20	24	22.8
Cloudflare	32	28	24	24	24	24	24	36	28	28	27.2
Google	8	16	48	48	104	16	8	44	12	12	31.6
Opendns	28	28	32	36	60	36	36	96	28	32	41.2
Cleanbrowsing	48	48	44	48	48	44	48	44	44	48	46.4
Quad9	40	48	48	44	44	48	52	44	52	60	48
Neustar	48	44	44	48	48	48	44	48	48	248	66.8
Freenom	44	80	48	48	80	500	48	92	44	48	103.2
Adguard	140	144	148	148	160	156	168	140	144	152	150
Comodo	156	148	148	148	148	148	152	156	152	148	150.4
Yandex	172	188	172	184	168	176	180	176	168	216	180
Norton	172	168	256	168	160	164	164	436	184	336	220.8
Level3	1000	44	1000	44	1000	44	40	44	44	44	330.4
1.1.1.2	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000

The RTT results were sorted out directly using the sort function command. For the ease of comparison we added a few more DNS providers other than the mentioned companies namely norton, neustar, adguard, level3, and freenom.

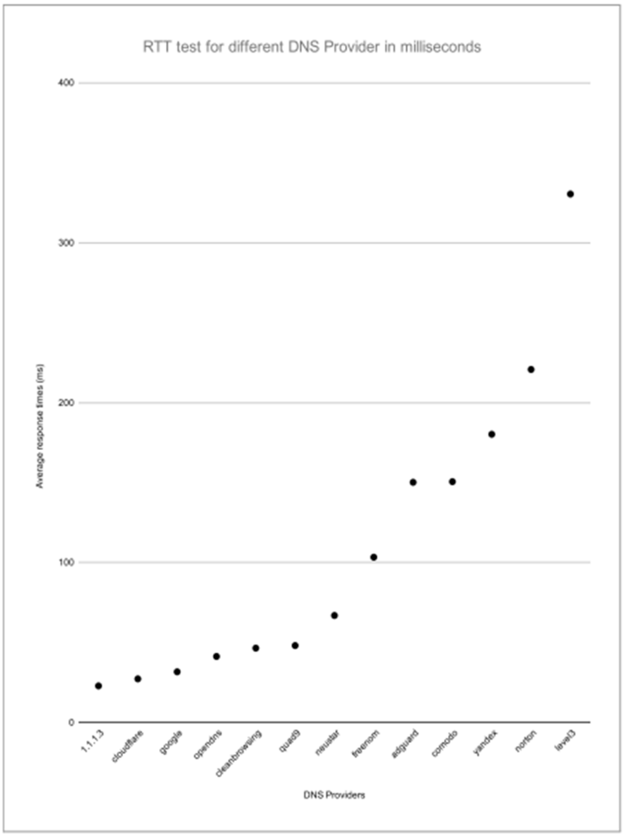


Figure 1 Average response times for different DNS providers

3.3Configuring proxy chains

Proxy Chains can be configured by editing the proxychains.conf file under the /eon any Linux based operating system. Any text editor like nano or vim can be used to modify this file but the user must have root privileges.

Before implementing we need to understand how different kinds of proxy chains work, Dynamic chain is one where all agents are chained accordingly as mentioned in the list, at least one agent must be online to play in the chain. All dead proxies are skipped, if all the proxies in the list are dead EINTR is returned to the app. In Strict chain all proxies mentioned in the list must be online for the request to go through else EINTR is returned to the app. Random chains are used to test the different proxies in the list and the system randomly selects one proxy and routes the traffic through that.

In this implementation we select the connection type as a dynamic chain (which is more flexible than a strict chain and is more reliable than a random chain). We then enter the details of the proxy server i.e., server type (socks4, socks5 etc.), IP address along with the port number, password (if any). Then we verify that the route back address is correct (127.0.0.1/8 for IPv4 and ::1/128 is the direct analog of the loopback range for IPv6) and save the file.

After editing the system file, we can run the proxy chains command by calling in the proxy chains followed by the application name (like a browser name) accompanied by a website Uniform Resource Locator (URL). The requests are routed through the proxies mentioned in the list and opens the specified URL in the application mentioned.

By default, the proxy chains run after the TOR exit node if the TOR service is online, in this case are not routing through TOR, hence we can leave TOR service offline and continue to test just the proxy chain.

4. Evaluation

A In this section we report and evaluate the level anonymity achieved by the user after current implementation of various measures on different platforms.

4.1 MAC Address Masking:

The MAC address spoofing was deployed on a Linux distro called Tails OS, (an Operating System that was previously discussed under Secure, Virtualized and temporary OS) running off of an 8 GB Pen drive with 7.53 GB Raw data storage utilizing a 150Mbps 2.4 GHz TP-Link nano TL-WN725N wireless network adapter with a permanent MAC address 50-3E-AA-53-7E-BD. Tails OS comes with all the basic utilities available on a Linux based operating system, after configuring the session, macchanger was deployed firstly to randomize the mac address manually.

Tails OS has an inbuilt MAC address randomizing function setting which by default sets the MAC address of the system to a random number.

The MAC address set by the system after the boot up was checked and noted down. After this it was compared using the Mac changer lookup tool to check its vendor and their MAC Address ranges and details.

After matching up the MAC address it was found that the MAC address generated by the Tails operating system was already randomized, through this check we verified and validated the default security measures setup by Tails OS to enrich your anonymity and privacy.

The Mac Address was then changed to fc:99:47:05:05:05 which comes within the range of a well-known vendors brand of routers. This was verified again using the ifconfig command in terminal. This system was then connected to a Wi-Fi router to check the MAC address from the routers side.

We noticed a device registered to a different brand rather than a TP link device on the router end. We performed another experiment by blocking the device through router settings to prevent the device for connecting to the Network. After changing the MAC address again in the Terminal using the Macchanger command it was observed that the device was able to connect to the router again using a different identity (MAC Address).

We also note that for any other Linux operating system we can use this Macchanger directly through the terminal if it is not available in the settings. Instead of Running this command each and every time we can add it to the crontab, this automatically randomizes the MAC address every time the system is booted. Macchanger is also available for windows and apple devices but the packages have to be downloaded separately.

4.2 Performance and Safety Evaluation of DNS resolvers:

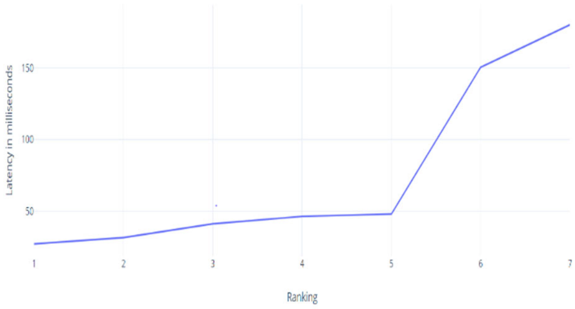


Figure 2 Graphical representation of DNS performance of the mentioned providers

Ranking for the best performed DNS provider in terms of RTT in descending order for the test location: Bangalore, India

1. Cloudflare 27.2 milliseconds
2. Google DNS 31.6 milliseconds
3. OpenDNS 41.2 milliseconds
4. Clean Browsing 46.4 milliseconds
5. Quad9 48 milliseconds
6. Comodo DNS 150.4 milliseconds
7. Yandex DNS 180 milliseconds

Table 2 Privacy options by different DNS providers

Providers	***Privacy***	***DNS Crypt***	***DNS over HTTPS***	***DNS Over TLS***
Google	Yes	No	Yes	Yes
Cloudflare	Yes	No	Yes	Yes
Quad9	Yes	No	No	Yes
OpenDNS	No	Yes	No	Yes
Clean Browsing	Yes	Yes	Yes	No
Yandex	No	No	No	No
Comodo	No	Yes	No	Yes

The Privacy option above is based on the providers pledge not to log or share the users DNS requests.

All providers other than Yandex performed well in South-East Asia. They all had under 50 milliseconds response time, which is impressive. In reality, a user can choose any one of these providers and won't even feel the latency variation.

- Cloudflare was the fastest DNS with only 27.2 milliseconds. And It also had an incredible average of 15 milliseconds across the world.
- Google and OpenDNS were close to second and third respectively. Cloudflare has a dominion and strong presence in the market. Whereas Google and OpenDNS had high response times from some locations.
- We cannot compare all these vendors in terms of one-on-one performance, since they all have specific features that can add some latency (Quad9 and Comodo blocks access to malicious domains, for instance).

As of 2020, we can say that Cloudflare has taken a dominant position in the DNS Market, providing the best of class DNS response times. They have their servers all over Europe, America, Asia, Russia giving them the upper hand when it comes to DNS. Compared to Google, they are providing free VPN with P2P encryption and DNS solutions for free. Having servers around the world enables them to provide free VPN based on the user's location. While there is an option for paid VPN, boasting much better encryption, carefully mapped routes to prevent Internet Traffic Jams, packet prediction, and privacy providing an IP from the United States. The free version provides an IP address from Turkey with comparatively lesser encryption grade and no Network traffic route management.

Recently, Cloudflare has also launched their DNS server for blocking malware (1.1.1.2) and for family safe usage (1.1.1.3), They are a great extension for 1.1.1.1 and give users, more options to as DNS filtering tools which was initially limited to Quad9 (For Malware) and Clean Browsing for Families.

Performance testing for 1.1.1.1/1.1.1.2/1.1.1.3, This was done by scrutinizing data for a domain that is not generally blocked by any of them(reddit.com), the obtained results were,

- 1.1.1.1: 27.2 milliseconds
- 1.1.1.2: 1000 milliseconds
- 1.1.1.3: 22.8 milliseconds

The numbers are close for 1.1.1.1 and 1.1.1.3, but exceptionally slower for the filtered services. Implying that, identifying domains in their blacklists does take a bit longer when they are being matched. Filtered or non-filtered DNS perform pretty much the same. Overall providing great performance [13].

4.3 Performance Evaluation of Proxy chans:

The RTT for the proxy chain is very high since it is being bounced off different proxy servers overseas and is routed back to the system. Hence the loading time for any website is really high, not to mention the latencies associated with it. For our test rig we used Kali Linux (A popular Linux distribution for penetration testing) on Oracle Virtual Box, since Kali Linux comes with all packages pre-installed. Allotted system resource for the VM was 6 cores at 3.8 GHz with 8 GB 2666 MHz RAM, with an ethernet adapter allotted for the VM specifically for the test. Wireless adapter was not used in this scenario as it would add up to some latency to the RTT even though it would be in terms of milliseconds. Also, Kali Linux supports very few wireless network adapters that are expensive and unconventional due to lack of driver support for most of them. WLAN adapters are not recommended until and unless the test involves network monitoring and wireless packet injection.

The tests involved lookups of DNS and IP addresses by using websites like duckduckgo.com and dnsleaktest.com, the main purpose of this test was to observe the requests going through the proxy servers mentioned in the list. And understand the impact of each hop on the response time. Geolocation checks were performed after successful completion of the chains to check our location through the IP address.

A DNS leak test was also conducted to check if there was a leak of the DNS request data. While using any privacy service, it is extremely important that all traffic produced by the user's computer is routed through the anonymizing network nodes. Traffic analysis can be conducted to analysis data leaks from the secure network connections, by any assailant monitoring the user's traffic can log all the activities [14].

Under certain conditions, even when the user is connected an anonymous network chain, the operating system will arbitrarily use the default DNS servers set by the developers, rather than the anonymous DNS servers assigned to your computer by the privacy service. DNS leaks are a crucial privacy threat since the anonymity network may be providing a false sense of security while data from private traffic is leaking.

5. Conclusion

All the preventive measures discussed in this paper can be taken with little to no prior experience. They will help the user to remain anonymous to a certain extent. Further study on this topic is needed to better understand and implement the concepts of internet privacy. Being anonymous has its own merits and demerits in an online society.

According to the tests performed, the web surfing experience will not be significantly affected by the implementation of MAC address masking or use of open DNS and any changes in the results can be attributed to fluctuations in the internet connection or due to the process of DNS query (which can be eliminated by performing the same test twice in which case the results are cashed at the local server and a DNS query is not needed). Based on these results, it is highly advisable for everyone to incorporate MAC address masking and using a DNS resolver of your choice into the daily web surfing activities.

The same is not necessarily true in the case of proxy chains as the results can vary drastically due to the nature of the service. So, although the use of proxy servers improves the privacy of the user in some cases, the trouble of identifying a trusted and reliable proxy server is just not worth the additional hassle for a general user. Most of the servers on the proxy chains are largely unregulated so there is a high chance that someone can use the information available there in not perfectly legal ways.

References

[1] Tarek S. Sobh, Yasser Aly, “Effective and Extensive Virtual Private Network,” Journal of Information Security, 2011, 2, pp. 39-49

[2] Dawson, Maurice & Cardenas-Haro, Jose , “Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance. International Journal of Hyperconnectivity and the Internet of Things,” pp. 47-55, IJHIoT.2017010104, 2017

[3] Rutkowska, Joanna. “Qubes OS Architecture,” 2010

[4] Sinha Sanjib,“Proxy Chains,” 2017

[5] Sungmo Jung, Jong Hyun Kim and Seoksoo Kim, “A Study on MAC Address Spoofing Attack Detection Structure in Wireless Sensor Network Environment,” ACN 2011, CCIS 199, pp. 31–35, 2011

[6] Alotaibi, Bandar; Elleithy, Khaled. 2016. "A New MAC Address Spoofing Detection Technique Based on Random Forests" Sensors 16, no. 3: 281.

[7] M. Anathi, K. Vijayakumar, “An intelligent approach for dynamic network traffic restriction using MAC address verification” Computer Communications, Volume 154, 2020, Pages 559-564, ISSN 0140-3664

[8] Henry Chukwuemeka Paul and Kinn Abass Bakon, “A STUDY ON IPv4 and IPv6: THE IMPORTANCE OF THEIR CO-EXISTENCE,” IJISE, Vol. 4 (No.2), November, 2016

[9] Sanjay, Balaji Rajandran and Pushparaj Shetty, “Domain Name System (DNS) Security: Attaacks Identification and Protection Methods,” Int'l Conf. Security and Management , SAM'18, pp. 27-33

[10] Robert Wahlstedt and Dr. Mercer, “Towards a Secure Deployment of DNS,” unpublished, December 11, 2019

[11] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso and Frank Piessens,“Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms,” AISA CSS ‘16, pp. 413-424

[12] Jung, Jaeyeon & Sit, Emil & Balakrishnan, Hari & Morris, Robert, “DNS Performance and the Effectiveness of Caching. ACM SIGCOMM Computer Communication Review,” 2002

[13] Labrador, Jeyran & Cruz, Michael & Dinawanao, Dante ,“DNSFilter: An Erlang/OTP Implementation of a DNS-Based Web Filtering System,” 2013

[14] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," 2005 IEEE Symposium on Security and Privacy (S&P'05), Oakland, CA, USA, 2005, pp. 183-195

[15] Renata Mekovec, “Onilne Privacy: Overview and Preliminary Research,” JIOS, Vol. 34, No. 2, 2010

[16] Nora McDonald, Benjamin Mako Hill, Rachel Greenstadt and Andrea Forte, “Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Service Providers” CHI 2019

[17] Balázs Bodó, “Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism,” INTERNET POLICY REVIEW Journal on internet regulation, Vol. 4, Issue 3