DOMAIN NAME SYSTEM POTENTIAL THREATS AND SECURITY MEASURES

[1]Prateek Gupta, [2]Himanshu Vishwakarma,[3]Keshav Raj Yadav,[4]Hriday Kumar Gupta
Computer Science and Engineering
KIET Group of Institutions,Delhi - NCR ,Ghaziabad,Uttar Pradesh, India
[1]prateek.2024cse1105@kiet.edu ,[2]himanshu.2024cse1160@kiet.edu,
[3]keshav.2024cse1187@kiet.edu , [4]hridaykumargupta@gmail.com

1. Abstract

The Domain Name System (DNS) serves as a critical component of the Internet infrastructure, translating human-readable domain names into IP addresses to facilitate communication between devices. However, its ubiquitous nature and fundamental role make DNS a prime target for various cyber threats. This paper comprehensively examines the potential threats faced by the DNS and explores effective security measures to mitigate these risks.

The research begins by elucidating the core functions of the DNS and its significance in enabling seamless Internet connectivity. Subsequently, it identifies and categorizes a range of threats that pose risks to the integrity, availability, and confidentiality of DNS services. These threats encompass DNS spoofing, cache poisoning, distributed denial-of-service (DDoS) attacks, DNS tunnelling, and domain hijacking, among others.
Moreover, the paper investigates the underlying mechanisms and attack vectors associated with each threat, providing insights into the tactics employed by malicious actors to exploit vulnerabilities in DNS infrastructure. Furthermore, it examines real-world case studies and incidents to illustrate the impact of DNS-related attacks on organizations and Internet users, emphasizing the importance of proactive security measures.
In response to these threats, the research evaluates a variety of security measures and best practices aimed at safeguarding DNS infrastructure and enhancing resilience against potential attacks. These measures include implementing secure DNS protocols (such as DNSSEC), deploying robust firewalls and intrusion detection systems, conducting regular vulnerability assessments and penetration testing, and fostering collaboration among stakeholders to share threat intelligence and coordinate incident response efforts.
Furthermore, the paper discusses emerging technologies and advancements in DNS security, such as threat intelligence platforms, anomaly detection algorithms, and blockchain-based DNS architectures, which offer novel approaches to address evolving threats and enhance the overall security posture of DNS infrastructure.
In conclusion, this research underscores the critical importance of DNS security in ensuring the stability and reliability of the Internet ecosystem. By raising awareness of potential threats and advocating for proactive security measures, this paper seeks to empower organizations and Internet stakeholders to effectively mitigate risks and protect against DNS-related cyber attacks.

2. Introduction

An essential as well as the crucial part of the internet is this DNS (Domain Name System), which links an unique IP address with a unique domain name that can be read by humans [17]. It helps in establishing the connection between the website and the user over the network by converting the Domain Name to numerical IP address. Instead of users memorizing complex IP address, they can use domain names like (www.something.com). There are some vulnerabilities of DNS to various threats due to which whether its functionality have been continuously challenged and based different issues over course of time. Given its primary purpose, it is not surprise that a wide variety of nefarious actions use the domain name service in one way or another. For example, spam emails contain URLs pointing to domains that, when resolved, lead to scam servers, and bots use DNS resolution to find their control servers and commands. Thus, it seems beneficial to

keep an eye out for clues in the DNS system that indicate a specific name is connected to nefarious activity.

In the vast network of the Internet, every device, ranging from personal smartphones and laptops to the powerful servers behind major online retail platforms, relies on numerical identifiers for communication. These unique numerical labels are known as IP addresses. Despite this reliance on numeric identification, accessing online content is made more user-friendly through the use of domain names. Instead of memorizing and entering lengthy numeric sequences, users can simply input a recognizable domain name, such as www.something.com, into their web browsers, effortlessly reaching their intended destination. Taking the example of something.com, when the user enters this in web browser, then a server working in background will undertakes the task of translating that human-friendly name into a numerical IP address, such as 1.2.3.4, associated with the specific domain. This whole process of translation is the fundamental function of DNS. When it comes to web browsing and other online activities like file transfers, DNS is crucial in providing the necessary information quickly so that users and remote hosts may connect.

The distribution of DNS mapping is organized in a hierarchical structure that spans the entirety of the Internet. Various authorities within this hierarchy collaborate to ensure the efficient and accurate resolution of domain names to their respective IP addresses.
Because of the Domain Name System's (DNS) critical role in networking, attackers are constantly looking for novel ways to compromise its infrastructure. Understanding the evolution of DNS security is essential to maintain reliable and secure services. Improving DNS security involves revising its design over time. Researchers have recently focused on enhancing DNS by incorporating necessary options and rethinking its operational assumptions. The attackers can swiftly move their infected system across different IP addresses by employing domain names. The fact that authorities may take down the domain name itself still presents a challenge for attackers. One common method to mitigate this danger is to include a domain generating algorithm into malicious programs, which allows the virus to communicate with an automatically generated domain name [10].

But the continued development of DNS and the appearance of new threats like ubiquitous adversaries, privacy hazards, and advanced attack methods emphasize how crucial it is to continue solving security, privacy, and functioning issues in DNS. The literature noticeably lacks a thorough assessment, summary, and classification of the body of work on DNS security and privacy that has already been done, despite efforts to enhance DNS design. This project is essential to help the community discover open issues that require further focus [5].

The Internet has become a crucial platform for communication as well as a major source of information and entertainment due to its extensive worldwide connectivity and large range of services. But there are additional security risks associated with this greater connectedness. Because the Internet is global in scope, security risks might appear out of the blue from any location in the world. In response to these risks, security experts employ a range of tactics, such as firewalls and antivirus software, which are successful in thwarting many attacks [11].

DNS hijacking is a common attack vector on the Domain Name System (DNS), garnering considerable attention and motivating efforts to strengthen defence mechanisms against such occurrences. One important factor in increasing awareness in this region has been the Sea-Turtle campaign. Numerous security research groups have disseminated information regarding these assaults, suggested countermeasures, and issued a warning that this may be a sign of more serious DNS-focused attacks.

DNS cache poisoning, in which erroneous data is introduced into a DNS cache to cause incorrect replies and users to be sent to inappropriate websites, is another danger to DNS architecture. The Delay Fast Packets (DFP) technique can help identify and stop this assault, which is also referred to as "DNS spoofing". Attackers seek opportunities to inject inaccurate records into the DNS cache. The DFP algorithm identifies and prevents attempts of cache poisoning attacks by analysing the distribution of round-trip times (RTT). In our model, assuming an eavesdropping attacker, the algorithm detects anomalies in the RTT, delaying the response and waiting for confirmation before allowing it to reach the DNS resolver. This helps prevent malicious responses from reaching users [1].

DNSSEC stands for Domain Name System Security Extensions which is a new protocol that is suggested to close the security holes. It mainly provides two security services to DNS: data integrity and source data authentication [2]. It uses digital public key cryptography and digital signature to efficiently implement these services. Together with the basic DNS records, this update adds new records (RR KEY, SIG, NSEC, and DS) for the purpose of keeping keys and signatures necessary for using a public key cryptography system [2].

DNSSEC has been used to improve DNS server security as part of Malaysia's efforts to fortify digital government security. This technology creates digital signatures inside DNS using cryptographic public keys. The DNSSEC standard was

introduced in 2005, but both the public and private sectors have not yet fully implemented it [4][5]. This article describes how the Malaysian government implemented DNSSEC on its domains as part of an effort to create a secure digital government. Supporting the country's digital economy and increasing public trust in government services are the goals [4][5].

3.CONCEPTUAL FRAMEWORK

3.1 DNS Overview

An essential part of the internet's architecture, the Domain Name System (DNS), converts human-readable domain names into IP addresses.
The smooth communication between devices connected to the internet is made possible by this mechanism. In order to maintain accessibility, dependability, and efficiency throughout the worldwide network, DNS is essential.

3.2 The Essential DNS Elements

3.2.1 Structure of Domain Names

Using the hierarchical structure of DNS, domain names are organized into tiers such as top-level domains (TLDs), second-level domains (SLDs), and subdomains [25]. One needs to be aware of DNS's structure in order to comprehend how it processes requests and directs internet traffic.

3.2.2 Domain Name Servers

There are several different kinds of servers in the DNS ecosystem, such as caching, recursive, and authoritative name servers. Every type of server contributes to the overall effectiveness and robustness of the system in a different way during the DNS resolution process.

3.2.3 Recording of Resources (RRs)

Resource Records are basic DNS data elements that hold details about a domain, including mail exchange servers, IP addresses, and other important data kinds. Analysing RRs' function sheds light on DNS's many features, which go beyond name-to-address mapping.

3.3 The Method of DNS Resolution

There are several processes involved in DNS resolution, from creating the first query to obtaining the IP address linked to a domain name. Examining the resolution procedure highlights the importance of DNS in preserving a reliable and effective internet infrastructure while also helping to sort out the intricacies involved.

3.4 Security Considerations in DNS

In the current internet environment, security is of utmost importance. This article explores the several security issues that DNS faces, such as cache poisoning, DNS spoofing, and distributed denial of service (DDoS) attacks. In order to counter these threats, it also introduces important security features like DNS Security Extensions (DNSSEC).

3.5 Changing Patterns and Technology

DNS changes as technology develops to meet new possibilities and problems. Two instances of contemporary trends that are described in this section are the adoption of DNS over TLS (DoT) and DNS over HTTPS (DoH). Their effects on privacy and security in the DNS environment are also highlighted.

4. OVERVIEW

4.1. VULNERABILITIES of DNS

Bellovin [11 , 12], Gavron [10], Schuba and Spaord [13], Vixie [14], discuss several security problems of DNS.

The two well-known issues that we discuss here are DNS Cache poisoning and the inability to validate DNS answers. The cache poisoning technique can be used by an attacker to force a name server P1 to query a different name server P2. An attacker may be able to get P2 to send back a DNS response with forged root records (RRs) if P2 is a hacked name server. If not, the attacker can transmit the DNS response to P1 while posing as P2 (see below). Remember that in order to enhance performance, a name server caches the outcomes of earlier exchanges with other servers. P1 might use the inaccurate DNS information provided by the attacker when resolving a name using its tainted cache. Most DNS implementations employ a weak message authentication method. An id is appended to a query by a DNS server (or a DNS client), which it then uses to compare with the associated response's id. Assume that a query is sent from server S1 to server P2. An attacker can send P1 a forged response with a corresponding query id if they can anticipate the query id that P1 will use. When P1 gets the response claiming to be from P2, P1 is unable to confirm that P2 is the source of the response. The attacker can pretend to be P2 and transmit the fake response to P1 if P2 isn't available when the query is submitted. In order to stop P2 from answering P1's inquiry, the attacker can launch a denial of service attack on P2 if it is up and running. Additionally, if a name server gets more than one answer to its query, it uses the first one. Therefore, if the forged response reaches P1 before P2's response does, the attacker can still succeed even if P2 is able to reply to P1 [1].

4.2. DNS CACHE POISONING

A cyberattack known as "DNS cache poisoning" tries to alter or tamper with the information kept in a DNS resolver's DNS (Domain Name System) cache. The DNS cache is used to store previously resolved domain name-to-IP address mappings, allowing faster retrieval of this information when requested by clients. When an attacker successfully poisons the DNS cache, they can redirect legitimate DNS queries to malicious IP addresses, leading to various security threats. Here's an overview of DNS cache poisoning: Attack Process: The forged DNS query is sends to a DNS resolver by the attacker. The query contains a malicious domain name and the attacker's chosen IP address. If the DNS resolver is vulnerable and does not properly validate the responses it receives, it may accept the attacker's response as legitimate and cache the malicious IP address associated with the domain [6].

If the information returned to a client waiting for a DNS answer has the correct DNS transaction ID, source port, and client address, the client will only accept it. These three bits of information are the only authentication mechanism that is used to obtain DNS replies. Finding the source IP is easy because we already know the address of the name server that has to be addressed. However, there is an issue with both the transaction ID and the source port. Because BIND regularly uses the originating port to reach the same name server, it is simple to locate. Actually, the only thing standing between the attacker and a successful cache poisoning is the transaction ID field in the DNS protocol. As a result, the attackers look for protocol implementation errors that would allow them to accurately calculate the transaction ID and stop transmission [1][7].

Consequences:

Redirected Traffic: Once the DNS cache is poisoned, all subsequent DNS queries for the poisoned domain name will be resolved to the attacker's IP address. This can lead to traffic being redirected to malicious servers.

Phishing: Another common Internet assault scenario is the creation of a phishing website by attackers, which is used to trick unwary users into divulging private information like credit card numbers and online banking credentials. The phishing website frequently mimics the appearance and feel of the intended legitimate website (such as an online banking service) and uses a similar-sounding domain name [8] .Attackers often use cache poisoning to redirect users to phishing websites that imitate legitimate sites, aiming to steal sensitive information [6].

Malware Delivery: Cache poisoning can be used to redirect users to malicious servers where malware is delivered to their devices.

Prevention and Mitigation:

DNSSEC: A collection of protocols intended to strengthen DNS security is known as DNS Security Extensions (DNSSEC). It makes it far more difficult for attackers to tamper with the cache by using digital signatures to confirm the legitimacy of DNS data [4].

Source Port Randomization: To make it more difficult for attackers to forecast the transaction IDs required to poison the cache, DNS resolvers can employ source port randomization [18].

4.2.1. Delay Fast Packets (DFP):Prevention of DNS Cache Poisoning

A method called Delay Fast Packets (DFP) is employed to stop DNS (Domain Name System) cache poisoning, which is a cyberattack that attempts to tamper with the information kept in a resolver's DNS cache. Malicious actors try to insert bogus DNS information into a resolver's cache in order to divert visitors to phony websites or intercept their communications. This technique is known as DNS cache poisoning.

DFP operates by causing timing inconsistencies or delays in resolvers' DNS response processing. The attacker's attempts to contaminate the DNS cache are thwarted by this delay mechanism, which interferes with their capacity to precisely forecast the time of valid DNS responses.

DFP can stop DNS cache poisoning in the following ways:

Randomized Delays: When processing DNS answers, DFP adds randomized delays. Resolvers purposefully induce various delays before processing and caching DNS responses, as opposed to reacting to queries instantly. Because these delays are erratic and differ for each query, attackers find it challenging to precisely timing their spoof answers.

Timing Pattern Obfuscation: DFP obfuscates the timing patterns that attackers use to carry out cache poisoning attacks by adding unpredictability to response times. The regularity of DNS response timings is often used by attackers to introduce fake

DNS records into the cache. When DFP is implemented, the timing signals become erratic, which makes the attack futile.

Dynamic Adjustment: Depending on a number of variables, including query trends, network load, and response times in the past, DFP may dynamically modify the delay parameters. This adaptable nature guarantees optimal performance under various circumstances and strengthens the DNS infrastructure's resistance to changing assault tactics.

Validation methods: DFP may use validation methods to confirm the legitimacy of DNS answers and ensure their integrity in addition to delay strategies. DNS records can be cryptographically signed using methods like DNSSEC (Domain Name System Security Extensions), which enables resolvers to verify the legitimacy of answers and identify any efforts at tampering.

Overall, by upsetting response timing predictability and strengthening DNS system resilience, Delay Fast Packets (DFP) offer an efficient defence method against DNS cache poisoning attacks. DFP contributes to maintaining the security and integrity of the DNS resolution process by using randomized delays and validation procedures [1][18].

4.3. DNS HIJACKING

DNS hijacking, a malicious activity synonymous with DNS redirection or DNS poisoning, presents a serious risk to the security and integrity of internet communications. In this exploitative maneuver, attackers intercept and modify Domain Name System (DNS) queries or responses, manipulating the translation of human-readable domain names to IP addresses. By gaining unauthorized control over DNS settings, attackers redirect legitimate domain requests to malicious websites, exposing users to phishing attacks and potential compromise of sensitive information. The methods employed for DNS hijacking vary, including compromising DNS servers, routers, or deploying malware on user devices. To fortify defenses against DNS hijacking, adopting robust security measures is imperative. Strategies such as the implementation of DNS Security Extensions (DNSSEC), utilization of encrypted DNS protocols, and routine monitoring and updating of DNS configurations are essential steps to bolster the overall security infrastructure of networks and protect against the risks associated with DNS hijacking[3].

Several of these worries reappeared with the start of the COVID-19 epidemic. Millions of people are now working from home, making VPN(Virtual Private Network) even more essential to the daily operations of many businesses [8]. This change brought attention to DNS-related VPN security vulnerabilities because the Sea Turtle campaign targeted VPNs as its main objective[15].

4.3.1. PREVENTION FROM DNS HIJACKING

DNSSEC: The IETF developed DNSsec to guarantee both the authenticity of the data's source and its integrity. DNSsec uses public key cryptography as its foundation to offer various security services [4]. As we've seen, the DNS is rife with errors, making it extremely open to attack.Transaction security of DNS communications, data security, integrity, authentication, and denial of service are a few of the security issues with DNS.The DNSSEC (Domain Name System Security Extensions) protocol is one possible solution for this security flaw. [2]. Two crucial security functions for DNS are provided by DNSSEC:Data integrity and source data authentication are guaranteed by DNSSEC. Public key cryptography and digital signatures are used by DNSSEC to effectively implement them. For usage in zone signing activities, two different types of keys are specified. Zone Signing Keys (ZSK) are the first kind, and Key Signing Keys (KSK) are the second.In addition to the original DNS records, this update uses new records (RR KEY, SIG, NSEC, and DS) to maintain keys and signatures that are required to use a public key cryptography system [2].
As we've covered and demonstrated above, the DNSSEC protocol offers authentication and data integrity, which has addressed many security issues with the DNS system. It is still vulnerable to several types of attacks, though. The total size of the DNSSEC zone file increases seven times over a DNS file when resource records are added to secure transactions [2]. Additionally, TCP rather than UDP will be used by the DNSSEC protocol. The network load will rise as a result of this.

4.4 *DNS MAPPING THREATS*

Websites that use DNS mapping to map multiple routes of their server catering users to connect their defined domain names with their services can create loopholes in the server for attackers to either increase the load on the server with DoS attacks or redirecting users to spam or unwanted sites by spoofing.

With these multiple domain names registered for mapping to a particular server component attacker can also use DNS tunnelling that involves encapsulating data within DNS queries or responses to bypass network security controls and exfiltrate sensitive information from a network. Attackers can abuse DNS protocol to

establish covert communication channels with command-and-control servers, enabling data exfiltration, malware propagation, or remote access to compromised systems.

Multiple domain mapping can be used to distribute malware by redirecting users to compromised websites hosting malicious software. Attackers can exploit vulnerabilities in DNS servers or compromise DNS records to redirect users to site hosting malware-infected files, leading to unauthorized installation of malicious software on users devices.
When multiple domains are mapped to templates of a server, it's essential to implement robust security measures to reduce threats and protect both the server and the domains. Here are several measures you can take:

4.4.1 *Ensure relevant Access Controls:*

Ensure that access to the server and its configuration settings is restricted to authorized personnel only. Implement strong authentication mechanisms, such as multi-factor authentication (MFA), and periodic review and update user access permissions to prevent unauthorized access.

4.4.2 *Secure configuration of the Web Server:*

Configure the web server securely by disabling unnecessary services, limit access to sensitive directories, and use secure protocols such as HTTPS to encrypt traffic between the server and clients.

4.4.3 *Define Network Segmentation:*

Segment the network to isolate the server hosting the templates from other critical systems and services like dynamic porting and controller action. This limits the potential impact of a security breach on other parts of the network and helps contain and mitigate attacks targeting the server.

4.4.4 *Regular Security Audits and Penetration Testing:*

Try ethical breaking into the system to discover the loopholes in the system that are particularly unforeseen. Perform thorough security assessments of the server configuration, web applications, and network architecture to uncover potential security weaknesses.

4.4.5 *Implement Intrusion Detection and Prevention Systems (IDPS):*

Use IDPS tools to keep an eye on network activity and spot any unusual or malicious activity directed at the server or any of its hosted domains. Configure the IDPS to alert administrators about potential security incidents and automatically block or mitigate identified threats.

4.5. DNSSEC IN THE MALAYSIAN GOVERNMENT DOMAIN

Malaysia is implementing DNS Security Extensions (DNSSEC) utilizing a multipronged approach to enhance the security and integrity of the internet infrastructure [30]. Efforts are made to inform stakeholders—such as government organizations, internet service providers, and domain registrars—about the benefits of DNSSEC and the possible dangers posed by DNS vulnerabilities, starting with an awareness campaign[5]. DNSSEC adoption is supported by a regulatory framework that is developed by organizations like the Malaysian Communications and Multimedia Commission (MCMC). Initiatives to increase capacity are carried out concurrently in order to provide IT workers with the abilities required for DNSSEC implementation. This covers technical assistance, training courses, and workshops. To promote widespread use, it is imperative to modernize DNS infrastructure, work with ISPs and registrars, and incorporate DNSSEC into domain registration procedures. In July2019, the Cabinet Notes included information about the deployment of DNSSEC on Malaysian government domains. This includes every.gov.my domain that belonged to the State Government, the Ministry, and its affiliated organizations [19]. By implementing DNSSEC in an effective manner and fostering a safe online environment in Malaysia, a comprehensive strategy is facilitated by ongoing monitoring, reporting procedures, and public education initiatives. International cooperation enhances the work even further and helps the nation stay current with DNS security concerns and best practices around the world.

Implementing DNSSEC required about a year and involved 439 domains in all. The level of security is increased by the deployment of DNSSEC on .gov.my domain names, and this has a big impact on the digital transactions and transformation that the Malaysian government offers to its citizens[5].

7. REFERENCES

[1] S. Cheung and K. N. Levitt, "*A Formal-Specification Based Approach for Protecting the Domain Name System*" IEEE, pp.6, NY, New York, USA,August 06, 2002.

[2] Seifert, C. Welch, I., Komisarczuk, P., "*Identification of Malicious Web Pages Through Analysis of Underlying DNS and Web Server Relationships*" in Proceedings of the 4th IEEE LCN Workshop on Network Security,pp.1-10 Victoria University of Wellington, 2008.

[3] R. Houser and S. Hao, "*A Comprehensive Measurement-based Investigation of DNS Hijacking*" in Proceedings of IEEE Conference, Chicago, IL, Publisher: IEEE. Affiliation: University of Delaware (R. Houser), Old Dominion University, 22 November 2021..

[4] K. Chetioui, G. Orhanou, S. El Hajji, and A. Lakbabi, "*Security of the DNS Protocol: Implementation and Weaknesses Analyses of DNSSEC*" in IJCSI International Journal of

Computer Science Issues, vol. 9, no. 2, issue 3, March 2012, pp. 6 , 13 figures. Laboratoire Mathématiques, Informatique et Applications, Université Mohammed V – Agdal.

[5] A. S. Abdullah, S. H. Marjuni, and M. Mukhtar, "*The implementation strategy of DNSSEC in strengthening digital government security in Malaysia*" Asia-Pacific Journal of Information Technology and Multimedia, vol. 11, no. 1, pp. 26-38, 2022.

[6] 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 (CCS '21), Virtual Event, Republic of Korea, Nov. 15-19, 2021, pp. 1-15. ACM, New York, NY, USA.

[7] Shimrit Tzur-David Kiril Lashchiver Danny Dolev Tal Anker School of Computer Science The Hebrew University Of Jerusalem "*Delay Fast Packets (DFP): Prevention of DNS Cache Poisoning*",School of computer science The hibrew university of jeruslem ,nov 2011,pp. 1-15,Israel.

[8] L. Bilge, E. Kirda, C. Kruegel, M. Balduzzi, "*EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis*" in Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, Feb. 6-9, 2011.

[9] Truong D., Cheng G. "*Detecting domain-flux botnet based on DNStraffic features in managed network*", Secur. Commun. Netw., (14) 9(2016), pp. 2338–2347.

[10] Bilge, L., Şen, S., Balzarotti, D., Kirda, E., & Krügel, C. (2014). "*Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains*" ACM Transactions on Information and System Security, 16(1), 14.

[11] S.M. Bellovin, "*Security Problems in the TCP/IP Protocol Suite*" Computer Communications Review, Vol.19, No.2, April 1989, pp.32-48.

[12] S. Bellovin, "*Using the Domain Name System for System Break-ins*" Proc. of the 5th UNIX Security Symposium, June 5-7, 1995, pp.199-208.

[13] C.L. Schuba, and E.H. Spafford, "*Addressing Weaknesses in the Domain Name System Protocol*" Technical Report, Department of Computer Sciences, Purdue University, 1994.

[14] P . Vixie, DNS and BIND Security Issues." Proc. of the 5th UNIX Security Symposium", June 5-7, 1995, pp.209-216.

[15] A. Kwan, "*Five Security Blind Spots from Prolonged Implementation of a Business Continuity Plan Amid COVID-19*," 2020. [Online]. Available: http://www.circleid.com/posts/20200225 five security blind spots from prolonged implementation of bcp/.

[16] Sainstitute, "*Attacking the dns protocol security paper*" 2003,pp.1-15.

[17] Tzur-David, S., Lashchiver, K., Dolev, D., Anker, T., "*Delay Fast Packets (DFP): Prevention of DNS Cache Poisoning*" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, pp. 28-41, Jan. 2012

[18] K. Chetioui, G. Orhanou, S. El Hajji, and A. Lakbabi, "*Security of the DNS Protocol - Implementation and Weaknesses Analyses of DNSSEC*" International Journal of Computer Science Issues (IJCSI), vol. 9, no. 2, issue 3, pp. 1-6, Mar. 2012.