International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

Domain Name System Security Extensions for Cyber Forensics

Seema S[1], Dr.Divya TL [2]

P.G. Student, Department of Master of Computer Applications, Rashtreeya Vidyalaya College of Engineering®, Mysore Rd, Bengaluru, India [1]

Assistant Professor, Department of Master of Computer Applications, Rashtreeya Vidyalaya College of Engineering® College, Mysore Rd, Bengaluru, India [2]

ABSTRACT: Domain Name System (DNS) reserve harming is a venturing stone towards cutting edge (digital) assaults. DNS store harming can be utilized to screen clients' exercises for control, to circulate malware and spam and to undermine accuracy and accessibility of Internet customers and administrations. As of now, the DNS framework depends on challenge reaction protections against assaults by (the normal) off-way enemies. Such safeguards don't get the job done against more grounded, man-in-the-middle (MitM), enemies. Be that as it may, MitM isn't accepted to be normal; consequently, there is by all accounts little inspiration to receive efficient, cryptographic components. We show that challengereaction don't ensure against store harming. Specifically, we survey basic circumstances where (1) aggressors can habitually get MitM abilities and (2) much more vulnerable assailants can sabotage DNS security. We likewise tentatively investigation conditions in the DNS foundation, specifically, conditions inside space enlistment centers and inside areas, and show that various conditions bring about increasingly helpless DNS. We audit space name framework security augmentations (DNSSEC), the protection against DNS store harming, and contend that not just it is the most appropriate instrument for forestalling reserve harming however it is likewise the main proposed barrier that empowers a posteriori scientific examination of assaults.

KEYWORDS: Domain Name System, Man-in-the-Middle Attack, Security augmentation, Cryptography, Malware

I. INTRODUCTION

DNSsec can be valuable for identification of assaults and in legal investigation. The element that makes this conceivable are advanced marks, which can be approved and confirmed by anybody with the ownership of an open confirmation key. Marks give a significant data to criminological investigation and can empower id, e.g., of the specific time that the system was assaulted and to which has the traffic was diverted. The typical security concern on conventional DNS system is cache poisoning. In most organizations, several official DNS full resolvers are constructed in order to provide name resolution services for the internal computers effectively since the cache function of DNS full resolvers can improve name resolution performance significantly.

Attackers target at those DNS full resolves and make them cache and provide malicious DNS information to querying clients. This kind of attacks are known as DNS cache poisoning. The marks likewise contain the tag of the cryptographic material (calculation, hash, key) that was utilized to create the mark. Notice that since the cryptographic marks should be difficult to manufacture for effective foes, just the substance possessing a cryptographic marking key, or a solid enemy with colossal computational force, ought to have the option to create legitimate marks. Therefore, a fashioned mark means that an extremely solid foe, for example, an administration, or a sign that the zone, which furnished the mock record with a substantial mark, might be pernicious or undermined.
In what follows, we think about how to break down assaults or recognize penetrates, performed by solid enemies, a posteriori. The paper proposes to use DNSsec to structure a framework that would empower examination of assaults, give confirmations of assaults that occurred and even empower discovery of certain assaults. The framework would need to gather the DNS reactions (alongside the comparing marks and cryptographic keys), e.g., by designing reasonable principles in the firewall, and store them in a database for preparing. The time stamps on the marks give a significant data, permitting to investigate when a specific mapping was viewed as legitimate, and when it comprises an assault. For example, consider an association that had a system square 1.2.3.0/24 and afterward moved to an alternate internet supplier and got another location square 5.6.7.0/24. Hence, reactions with mappings from the square 1.2.3.0/24

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

are not, at this point legitimate, and if a resolver on some system gets records with mapping from old square, this might be a sign of an assault.

II. RELATED WORK

In [1], the author discusses how the DNS protocol was considered as a secure communication protocol so that each computer connected to the Internet trusted received answers from DNS full resolvers. Therefore, malicious DNS response such as wrong IP address that belongs to a phishing site can be used by querying client. But later on [4] it has been discussed due to implementation errors DNSSEC protection may fail, even when both the resolver and zone deploy it: validation of signatures of important top level domains, e.g., mil, fails since the root does not delegate the public signature key of mil but instead provides an incorrect indication that mil does not support DNSSEC. Then the results in the resolvers will be falling back to a non-validating mode.
In [5], the principle three issues have been referenced and given an idea about it as the (I) since there exists a birthplace check to the reaction parcel in DNSSEC framework, which prompts data observing and crisis reaction work disappointment in current checking framework. (ii) the absence of help for the national trust stay brings about the results that DNSSEC trust chain can't be made in the framework, (iii) as conveying DNSSEC on the root area name server isn't as of now yet accessible, we will confront the issue of being not able to collaborate with remote servers.
In [2], the paper discusses the methods of beating the issue of any security issues. (I) Preventing Fragmentation with zone administrators and enlistment center, name servers. (ii) Preventing Defragmentation Cache Poisoning, can be practiced by setting more grounded limitations on the defragmentation support. (iii) Preventing DNS-harming by means of Spoofed second Fragments through resolver - irregular (length) prefix barrier and nameserver - arbitrary postfix resistance. At that point onwards, in [8], the paper tells this present reality perceptions of the issue with divided reactions. These perceptions result from organize follows recorded on a legitimate name server of SURFnet. This server is legitimate for±4000 zones, including±300 DNSSEC-marked zones. It receives±500 inquiries every second all things considered.

III. PROPOSED TECHNOLOGY

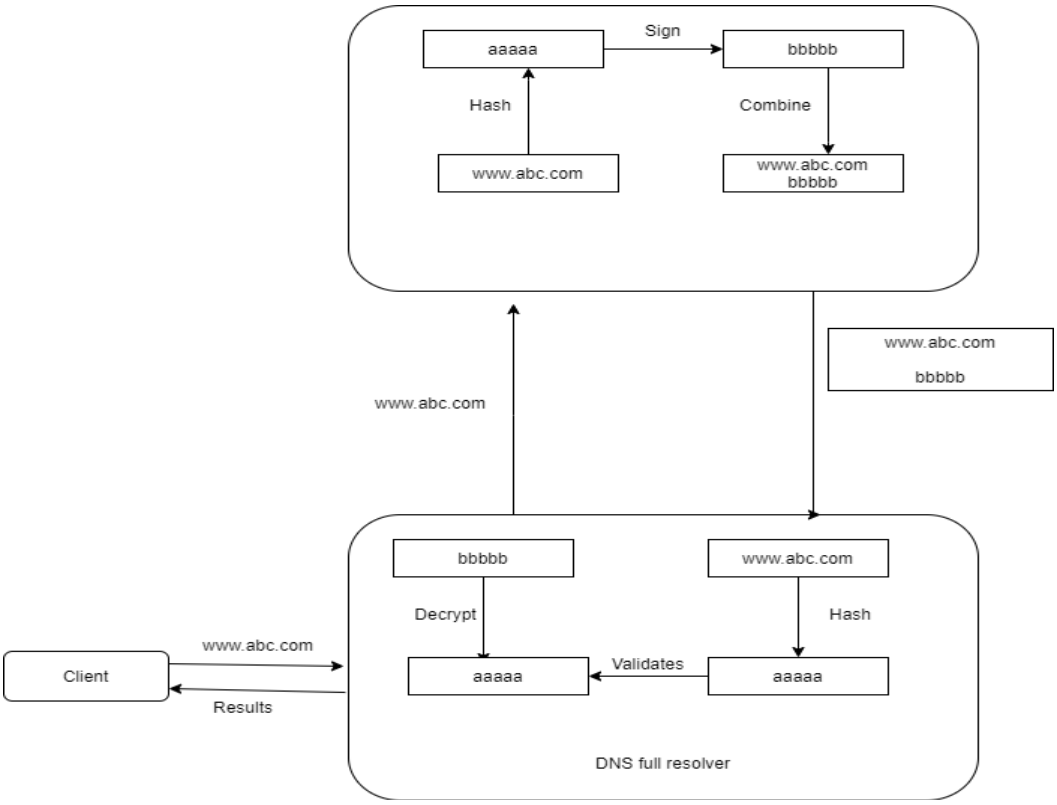

Fig 1. Overview of DNSSEC working

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

The above block diagram tells the working of a website with DNSSEC.

- The client sends a recursive query to its local recursive caching DNS server
- DNS server sends an iterative query to the root server. The root server responds with a referral net zone's name servers
- The recursive caching DNS sends an iterative query to the net zone server
- The net server responds with a zone name server. That zone server will respond with an IP address requested by the client after checking for originality
- Client can then interact with that IP address and the results will be returned to the client

Iterative query is the request to the DNS server where the client randomly asks for what is available in the web without asking for outer reference.

The recursive query is also a request to the DNS server where the client will be particular in what he wants with the help of external reference.

A DNS zone is implemented in the configuration system of a domain name server. It contains all the records in that particular zone.

The website give a wrong response to the client if it doesn't have a working DNS Security Extension.

The following process happens:

- The client sends a recursive query to its local recursive caching DNS server
- DNS server sends an iterative query to the root server. The root server responds with a referral net zone's name servers
- The recursive caching DNS sends an iterative query to the net zone server
- An evil DNS server responds with an IP address which is incorrect and not safe
- It poisons the cache and sends an evil website to the client. Then the client interacts with evil IP address which indirectly responds or performs a man-in-the-middle attack by passing and observing traffic from legitimate web server

IV. DEPLOYMENT OF DNSSEC

We have to remember that conveying DNSSEC is a two way process. DNSSEC must be sent at both the legitimate side (DNS servers) and the customer side (resolvers, programs, applications). At the customer side a definitive security will be accomplished if the DNSSEC approval is finished by the end-client applications as opposed to by outside resolvers at the ISP. OpenDNSSEC is an independent DNS zone underwriter that should work with a DNS server as long as the zones are record based. OpenDNSSEC is a PC program that deals with the security of area names on the Internet. The venture means to drive selection of Domain Name System Security Extensions (DNSSEC) to additionally improve Internet security. OpenDNSSEC was made as an open-source turn-key answer for DNSSEC. It makes sure about DNS zone information not long before it is distributed in a definitive name server. OpenDNSSEC takes in unsigned zones, includes computerized marks and different records for DNSSEC and gives it to the definitive name servers for that zone.

Intended for security first, Secure64 DNS arrangements are reason worked in light of flexibility. From the underlying foundations of our Secure OS to our strong DNS Guard instruments, Secure64 DNS servers start with security. Secure64 is a finished DNS and DNSSEC machine with an accentuation on security and robotization.

Tie is utilized effectively for each application from distributing the (DNSSEC-marked) DNS root zone and many top-level spaces, to facilitating suppliers who distribute exceptionally huge zone documents with numerous little zones, to ventures with both inner (private) and outer zones, to specialist organizations with enormous resolver ranches.

V. RESULTS

DNS resolution happens before a client ever collaborates with a site's application, and if DNS is captured, the client may wind up communicating with a sham site rather than the expected endpoint. Fruitful assaults can be incredibly destructive to mark notoriety, and the convention's forceful reserving engineering makes it hard to rapidly correct harmed records. Likewise, while DNSSEC approval might be undetectable to the end client today, programs may create straightforward methods for showing the augmentations' accessibility sooner rather than later. It is a lot of augmentations to DNS which give to DNS customer's cryptographic validation of DNS information, confirmed refusal of presence, and information respectability, yet not accessibility or classification. The component of DNSSEC is proposed to improve DNS security. DNSSEC gives protection from MitM foes by depending on cryptographic verification (signature) of records in reactions.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 5, May 2020 ||

VI. CONCLUSION

DNSSEC is a security system that gives DNS Servers the ability to verify that the information received is reliable. It also looks through to prevent the Denial-of-Service by protecting the integrity. With the help of this system, DNS spoofing can be removed as every information is checked before sending it to the client. It is necessary to use this security extension as it uses the digital signatures to strengthen the authentication. DNS Security Extension also helps in preventing the frauds in online E-Commerce business, which helps the business economically by making a high correctness and availability to the functions on the internet.

REFERENCES

[1] Kakoi, Kunitaka, et al. "Design and Implementation of A Client Based DNSSEC Validation and Alert System." 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2016.
[2] Herzberg, Amir, and Haya Shulman. "Fragmentation considered poisonous, or: Onedomain-to-rule-them-all. org." 2013 IEEE Conference on Communications and Network Security (CNS). IEEE, 2013.
[3] Herzberg, Amir, and Haya Shulman. "Towards Adoption of DNSSEC: Availability and Security Challenges." IACR Cryptology ePrint Archive 2013 (2013): 254.
[4] Herzberg, Amir, and Haya Shulman. "Security of patched DNS." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2012.
[5] Sun, Yu, Ru Juan Liu, and Yi Liu. "Research and implementation of DNSsec monitoring system." 2010 International Conference on Machine Learning and Cybernetics. Vol. 4. IEEE, 2010.
[6] Jin, Yong, Masahiko Tomoishi, and NariyoshiYamai. "An advanced client based DNSSEC validation and evaluations toward realization." 2016 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2016.
[7] Pappas, Vasilis, and Angelos D. Keromytis. "Measuring the deployment hiccups of DNSSEC." International Conference on Advances in Communications. Springer, Berlin, Heidelberg, 2011.
[8] Van Den Broek, Gijs, et al. "DNSSEC meets real world: dealing with unreachability caused by fragmentation." IEEE communications magazine 52.4 (2014): 154-160.
[9] Mohaisen, Aziz, ZhongshuGu, and Kui Ren. "Privacy implications of DNSsec look-aside validation." 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017.
[10] Yan, He, et al. "Limiting replay vulnerabilities in DNSsec." 2008 4th Workshop on Secure Network Protocols, IEEE, 2018