



A survey on Domain Name System Security

¹Ms. Maitri Patel, ²Dr. Rajan Patel

¹Research Scholar

Faculty of Engineering & Technology

Sakalchand Patel University, Visnagar

Email: maitru1487288@gmail.com

²Associate Professor

Department of Computer Engineering

Sakalchand Patel University, Visnagar

Email: rajanpatelce@gmail.com

Abstract

DNS (Domain Name System) represents mapping between domain names and their numerical identifiers. DNS designer has not taken care about security issues related to DNS in the beginning as main goal to develop DNS is to provide mapping. With wide spread and usage of internet, DNS is one of the most vital component for internet now a days. In daily internet usage like accessing e-mails, website surfing or using chat applications, DNS plays major role for every internet user. Also, many other protocols depend on its function. Thus, various cyber-attacks like denial of service attack, cache poisoning, malicious domain names etc. are being done on DNS and security of DNS has been continually challenged due to its vulnerability to these cyber-attacks. DNS vulnerability may lead to access of wrong websites or no access to websites. That can cause a huge economic loss for the user. In this paper, Survey on DNS security has been performed to identify the types of attacks possible on DNS. Also, Survey on various DNS security systems has been performed based on protection they are giving against cyber-attacks. Among of them, detailed analysis has been performed on DNSSEC (DNS Security Extension), an extension to the original DNS protocol proposed in RFC 2535 (later updated in RFC 3007, 3008 and 3090) that provides authentication and integrity for the data transferred by DNS. DNSSEC uses public key cryptography to provide authentication and integrity for the data transferred by DNS. Existing public key cryptographic algorithms like RSA (Rivest Shamir Adelman Algorithm) and ECC (Elliptic Curve Cryptography) are used by DNSSEC to provide authenticity and integrity of data transferred by DNS. Analysis and comparison of these algorithms has been performed based on various factors used for public key cryptography. Also, advantages and disadvantages of using ECC in DNSSEC has been discussed. Finally, DNS security future aspects has been discussed.

Keywords: DNS; Security; RSA; ECC; DNS Vulnerability; DNSSEC

1. Introduction

DNS, a globally distributed dynamic database is mainly composed with domain name space and resource records, name servers and resolvers^[1]. Hostnames, understand by humans are converted into IP addresses, understand by machines with the use of DNS^{[1], [2], [3], [4]}. If DNS will not work properly, huge part of internet will get impacted. Thus, DNS is crucial part of internet infrastructure^{[5], [6], [7]}. Primarily DNS was not designed to provide security, it is considered to be more vulnerable against cyber-attack. As one of the main attraction for cyber terrorist is to find out DNS vulnerability, it is essential to provide DNS security.

1.1. Architecture of DNS:

Domain Name (a symbolic string associated with an IP address), Domain Name Space (referred as a hierarchy in the internet naming structure) and Name Server are the main components of DNS architecture.

Figure 1 shows tree structure for DNS domain name space database. The empty label represents DNS (root of the tree). Many management spaces has been allotted to divide the domain name space into zone [9], [10].

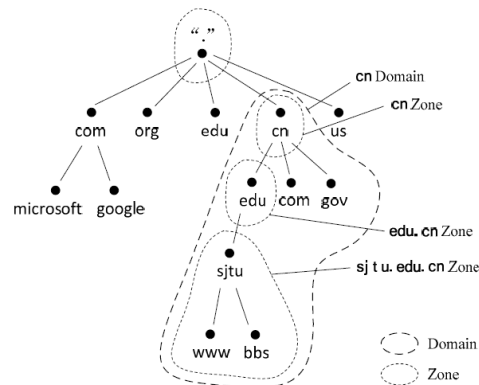


Figure 1. Hierarchical Structure of DNS

1.2. Working of DNS:

Domain name gives precise information to empower web browsers to spot particular web page. To perform mapping of domain name with IP address, DNS server first ask the root domain name server that returns IP address of the authoritative name servers. There are 13 root server available in the world at this time. Authoritative DNS name servers provides answers to recursive DNS name servers with IP “mapping” of particular website. Recursive DNS name servers are authorised for providing the proper IP address of particular domain name to the requesting host. Figure 2 represents resolution process for DNS assuming that user needs to parse the domain name of `www.test.com` [10], [11].

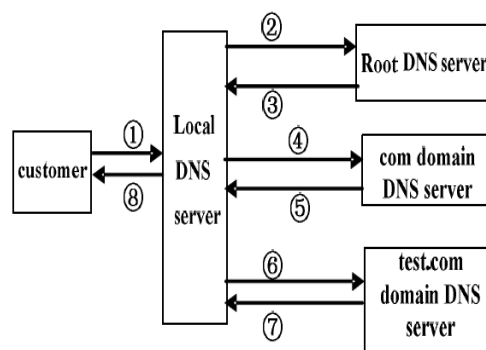


Figure 2. Resolution Process for DNS

The structure of remaining paper is as follows: In Section 2, vulnerabilities of various DNS protocol has been discussed. Section 3 presents survey on existing security protocols implemented to provide DNS security against various type of attacks. In Section 4, detailed analysis on DNSSEC protocol, used to provide authenticity has been performed. Conclusions are being presented in Section 5.

2. DNS Protocol Vulnerability

Many factors are used to determine DNS vulnerability. RFC 882 and RFC 883 are first DNS protocols designed in 1983. The security issues has not been taken into consideration at that time. A serious defects in DNS protocol was found by Steve Bellovin in 1990. The DNS servers in internet uses simplex software. ISC BIND software is mostly used by most DNS servers. The up gradation for ISC BIND software has been slow by administration.

First execution of DNS, C language implementation and open source are the main three factors that are responsible for the problem in BIND^[12]. The latest version for BIND (v9) is implemented from scratch to deal with all these problems^[12]. Significant improvement is there, but still flaws can be found in it^[12]. Security vulnerabilities are not just found in BIND. But they can also be found in protocols implemented much later than BIND such as Windows DNS^[12].

Security flaws found in DNS are DOS (Denial of Service - A specially formatted query is sent by a client to crash the server), RCE (Remote Code Execution - The attacker takes the control to DNS on target machine by sending unusual query that diverts flow of execution to some mischievous code), Cache Poisoning or Spoofing (Improper or inappropriate information is injected inside the target machine's DNS to lead astray the traffic to the destination selected by the attacker in place of correct destination), Protocol weaknesses (Inherent security pitfalls in DNS protocol and algorithms are exploited) etc.^[12].

3. Survey on Existing DNS Security Systems based on various type of attacks:

Sr No	Proposed Method	Methodology Used	Security Services	Attack Detection	Attack Prevention	Type Of Attack/ Problem	Remarks
1	Measurement Study ^[3]	Signed domains of DNSSEC dataset are measured and potential for amplified DDoS attacks are compared with the representative domains that do not implement DNSSEC	Authentication and Integrity	No	Yes	Cache poisoning attack	Use of DNSSEC for authenticity, makes larger responses. Also, if ANY-queries are considered, DNSSEC-signed domains yield high amplification factors
2	Kopis System ^[6]	Detects malware domains at upper DNS hierarchy by monitoring network traffic	Integrity	No	Yes	Malware attacks	It can detect malware domains even when no IP reputation information is available

3	S-DNS ^[8]	Decreases the success probability of DNS spoofing and cache poisoning by preventing man-in-the-middle attacks and provides backward compatibility and simple security solution with low computation and communication overheads.	Integrity	No	Yes	Cache poisoning attack	Protocol cooperates with Identity Based Encryption server for preventing cache poisoning attack
4	A practical approach to distinguish between valid and bogus DNS replies ^[13]	Uses iptables and routine fail2ban detection	Authentication	No	Yes	DDoS attack	Focuses only on prevention of amplify DDoS attack. Other types of DNS attacks are not taken into consideration
5	ADNS using Chord Protocol ^[14]	Primary and secondary servers are main components of the system. Primary servers and secondary servers built special network for the region they are authorised.	Availability	No	Yes	Load balancing problem and Single point failure problem of existing DNS	Consumes a high network bandwidth compare to traditional DNS
6	T-DNS ^[15]	Uses TCP and Transport layer security to provide DNS security	Consistency	No	Yes	Amplified DDoS attacks	Use of TCP, improves privacy and security of DNS as compare to UDP

7	Anax, DNS protection system ^[16]	Uses Anax poisoning detection engine and database to identify cache poisoning attack in cached DNS records	Integrity	Yes	No	Cache poisoning attack	Detects cache poisoning attack locally in cache records only. Fully automated
8	DNS proxy Countermeasure ^[17]	Uses DNS proxy server(DPS) and BIND	Integrity	Yes	Yes	Cache poisoning attack	No change in DNS standards. Performance impact is minimal
9	CGA-TSIG algorithm ^[18]	Public key cryptography is being used to form a connection with DNS server. Extends RDATA field of TSIG to implement security	Authentication	No	Yes	DNS spoofing	Developed for stateless auto configuration in IPv6 as DNSSEC and TSIG protocols were not able to deal with stateless configuration in IPv6
10	Self-feedback correction system ^[19]	Provides correct mapping between domain name and IP address for DNS wrong resource records	Integrity and Authentication	No	Yes	Malware attacks	Uses webpage fingerprint algorithm as one parameter to provide correct mapping of domain name and IP address that not works for https
11	Exposure system ^[20]	Domains that are concerned for performing malicious activity are being identified	Integrity	No	Yes	Malware attacks	More efficient compared to Notos as it uses time-based features to detect malicious domains

12	Domain Watcher System ^[21]	Malicious domains are being identified using local and global textual features. Introduces new global textual features-imitation features and bigram features	Integrity	No	Yes	Malware attacks	Lightweight system and efficient compared to other systems
13	Notos ^[22]	Forms models of authorised domains and malicious domains. This models are used to specify whether the new domain is malicious or legitimate by computing reputation score	Integrity	No	Yes	Malware attacks	Domains represented with new address space each time and not used again for other malicious purposes are not being identified

Table 1. DNS Security System

4. Detailed analysis of DNSSEC

DNSSEC protocol is not fully deployed^{[23], [24], [25]}. A partial implementation of DNSSEC exists today. DNSSEC protocol provides authenticity^[26] and integrity^[26] of data transmitted by using algorithms like SHA-1^[27], RSA^{[28], [29]} and ECDSA^[30]. In DNSSEC, RSA/MD5 and DSA (Digital Signature Algorithm) are used for the purpose of authenticity. Digital signatures can be generated by public key algorithms. It can be verified by the authorised person with use of public key. For security purpose, ECDSA is growing in industry to provide authenticity now a days.

With increasing use of technology, mobile phones are being commonly used by everyone to scrutinise E-mails or to visit invulnerable site on internet. To provide security, RSA and ECC public key algorithms has been used. ECC and RSA provides similar level of security. But as compared to RSA, ECC gives some advantage over RSA like small key size, faster computation, and memory and energy savings^[31].

[1] Small Key Size and Faster Computation:

In 124-bit RSA, Modular exponentiations of large integers are used as RSA operations and factorization of these large integers has been used to provide security. In 160-bit ECC, groups of points over elliptic curves are used as ECC operations and discrete logarithm problem (ECDLP) is used to provide security. Both algorithms provide the same security.

But, use of elliptic curve and ECDLP are the main reasons that permits ECC to have similar security level with advantages of small key size and greater computational efficiency.

[2] Memory and Energy savings:

Algorithm which suits more for handheld and mobile devices is ECC as it needs fewer power for its functioning with use scalar multiplications. In scalar multiplication, additions has been performed and intermediate results are not getting stored. Thus, it requires less use of registers and memory space.

In RSA, multiple precision multiplication is performed of large integers. Thus, it requires more energy compared to addition operations perform in ECC. Since limited number of registers are available, it requires more data transfer to and from memory to store data.

4.1. Comparison of ECDSA and RSA algorithms:

4.1.1. Following is the comparison of parameters for RSA and ECDSA algorithms used for DNS [31], [32], [33]:

Parameters	ECDSA	RSA
Key Size (same security)	192 bit length Smaller	1024 bit length Bigger
Signature Generation	Fast	Slow
Signature Verification	Slow	Fast
Encryption	Slow	Fast
Decryption	Fast	Slow
Key Exchange	Slow	Slow

Table 2. ECDSA vs. RSA

4.1.2. Following is the comparison for signature validation speed between RSA and ECC [34]:

ECC Algorithm	OpenSSL Version ⁺	Compared To*			
		RSA		ECDSA	
		1024	2048	P-256	P-384
ECDSA P-256	0.9.8zh	27.5	8.4	-	-
	1.0.1f	26.0	7.9	-	-
	1.0.2e	11.5	3.6	-	-
ECDSA P-384	0.9.8zh	57.7	17.6	-	-
	1.0.1f	77.6	23.4	-	-
	1.0.2e	87.3	27.2	-	-
Ed25519	(1.0.2e) ⁺	7.9	2.5	0.7	0.1
Ed448	(1.0.2e) ⁺	23.4	7.3	2.0	0.3

Table 3. Comparison for Signature Validation Speed for RSA and ECC

5. Conclusion

According to survey performed, there are various DNS security systems and protocols are available to provide security against various cyber-attacks. DNSSEC protocol provides authenticity and integrity of data transmitted by using algorithms like SHA-1, RSA and ECDSA. But, DNSSEC protocol is not fully deployed. Also, there is not any security system or protocol that provides confidentiality for the data transmitted by DNS. Most of the security system or protocol uses public key cryptography. Public

key cryptography has drawbacks like certification problem, direct compromise, false sense of security and speed. Thus, there is a need of security system or protocol that can provide confidentiality, integrity and authenticity for the data transferred by DNS and also that can overcome the drawback of public key cryptography.

References:

- [1] Fangming ZHAO, Yoshiaki HORI and Kouichi SAKURAI, Analysis of Existing Privacy-Preserving Protocols in Domain Name System, IEICE Transactions. 93-D. 1031-1043. 10.1587/transinf.E93.D.1031., Online ISSN: 1745-1361.
- [2] M.H.Jalalzai, W.B. Shahid and M.M.W. Iqbal, DNS security challenges and best practices to deploy secure DNS with digital signatures, IEEE-2015, Electronic ISBN: 978-1-4799-6369-0, DOI: 10.1109/IBCAST.2015.7058517.
- [3] Roland van Rijswijk-Deij, Anna Sperotto and Aiko Pras, DNSSEC and its potential for DDoS attacks: a comprehensive measurement study, ISBN: 978-1-4503-3213-2, DOI:10.1145/2663716.2663731.
- [4] Eric Osterweil, Dan Massey and Lixia Zhang, Deploying and Monitoring DNS Security (DNSSEC), Print ISSN: 1063-9527, DOI: 10.1109/ACSAC.2009.47
- [5] Amir Herzberg and Haya Shulman, DNSSEC: interoperability challenges and transition mechanisms, IEEE -2013, Electronic ISBN: 978-0-7695-5008-4, DOI: 10.1109/ARES.2013.53.
- [6] Manos Antonakakis, Roberto Perdisci, Wenke Lee and David Dagon, Detecting malware domains at the upper DNS hierarchy, August-2011, 27-27.
- [7] Andrew J. Kalafut, Craig A. Shue and Minaxi Gupta, Touring DNS open houses for trends and configurations, Journal of IEEE/ACM Transactions on Networking (TON), DOI:10.1109/TNET.2011.2130537.
- [8] Ramzi Bassil, Roula Hobeica and Wassim Itani, Security analysis and solution for thwarting cache poisoning attacks in the domain name system, IEEE -2012, Electronic ISBN: 978-1-4673-0747-5, Print ISBN: 978-1-4673-0745-1, Online ISBN: 978-1-4673-0746-8, DOI: 10.1109/ICTEL.2012.6221233.
- [9] Futai Zou, Siyu Zhang and Bei Pei, Survey on domain name system security, IEEE-2016, Electronic ISBN: 978-1-5090-1192-6, DOI: 10.1109/DSC.2016.96.
- [10] Amy Friedlander, Allison Mankin, W. Douglas Maughan and Stephen D. Crocker, DNSSEC: a protocol toward securing the internet infrastructure, DOI:10.1145/1247001.1247004. Eric Osterweil, Dan Massey and Lixia Zhang, "Deploying and Monitoring DNS Security (DNSSEC)", IEEE-2009, DOI: 10.1109/ACSAC.2009.47.
- [11] Shao Ming-zhu, Sun Bo and Xie Rui-yun, The Research of DNS Safe Analysis and Defense Technology, ISSN: 2194-5357, DOI: https://doi.org/10.1007/978-3-642-31656-2_138.
- [12] Martin Carlisle and Barry Fagin, IRONSIDES: DNS with no single-packet denial of service or remote code execution vulnerabilities, IEEE-2013, DOI: 10.1109/GLOCOM.2012.6503217.
- [13] Muhammad Yeasir Arafat, Muhammad Morshed Alam and Feroz Ahmed, A Realistic Approach and Mitigation Techniques for Amplifying DDOS Attack on DNS, Proceedings of 10th Global Engineering, Science and Technology Conference 2-3 January, 2015, BIAM Foundation, Dhaka, Bangladesh, ISBN: 978-1-922069-69-6.
- [14] Shidong Zhang, Gengyu Wei and Bai Wang, The design and implementation of an alternative domain name system, IEEE-2010, DOI: 10.1109/ICBNMT.2010.5704869.
- [15] Liang Zhu, Zi Hu and John Heidemann, Connection-Oriented DNS to Improve Privacy and Security, IEEE-2015, DOI: 10.1109/SP.2015.18.
- [16] Manos Antonakakis, David Dagon, Xiapu Luo, Roberto Perdisci, Wenke Lee and Justin Bellmor, A centralized monitoring infrastructure for improving DNS security, ISBN: 3-642-15511-1 978-3-642-15511-6, DOI: https://doi.org/10.1007/978-3-642-15512-3_2.
- [17] Jonathan Trostle, Bill Van Besien and Ashish Pujari, Protecting against DNS cache poisoning attacks, IEEE-2010, DOI: 10.1109/NPSEC.2010.5634454.
- [18] Hosnieh Rafiee and Christoph Meinel, A Secure, Flexible Framework for DNS Authentication in IPv6 Autoconfiguration, IEEE-2013, DOI: 10.1109/NCA.2013.37.

- [19] Caiyun Huang, Peng Zhang, Junpeng Liu, Yong Sun, Xueqiang Zou, SFCSD: A Self-Feedback Correction System for DNS Based on Active and Passive Measurement, arXiv: 1704.06569 [cs.NI].
- [20] Leyla Bilge, Engin Kirda, Christopher Kruegel and Marco Balduzzi, EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis, January 2011.
- [21] PanpanZhang, TingwenLiu, YangZhang, JingYa, JinqiaoShi and YubinWang, Domain Watcher: Detecting Malicious Domains Based on Local and Global Textual Features, DOI: <https://doi.org/10.1016/j.procs.2017.05.204>.
- [22] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee and Nick Feamster, Building a Dynamic Reputation System for DNS, USENIX Security'10 Proceedings of the 19th USENIX conference on Security, Pages 18-18, and ISBN: 888-7-6666-5555-4.
- [23] Mark Ravis, Eleana Asimakopoulou and Stelios Sotiriadis, Addressing Complexity in DNS Security: A Case for Improved Security Status Indication Based on a Trust Model, IEEE-2013, DOI: 10.1109/3PGCIC.2013.78.
- [24] Nicholas A Plante, Practical Domain Name System Security: A Survey of Common Hazards and Preventative Measures.
- [25] Mohammed Abdulridha Hussain, Hai Jin, Zaid Alaa Hussien, Zaid Ameen Abduljabbar, Salah H. Abbdal and Ayad Ibrahim, DNS Protection against Spoofing and Poisoning Attacks, Electronic ISBN: 978-1-5090-2535-0, DOI: 10.1109/ICISCE.2016.279
- [26] Suranjith Ariyapperuma and Chris J. Mitchell, Security vulnerabilities in DNS and DNSSEC, Print ISBN: 0-7695-2775-2, DOI: 10.1109/ARES.2007.139
- [27] Tanmay Chattergee, Configuration of DNS server with cryptographic algorithm for secure DNS and DHCP updates, IEEE-2012, DOI: 10.1109/ICCCNT.2012.6395990. Roland van Rijswijk-Deij, Mattijs Jonker and Anna Sperotto, On the adoption of the elliptic curve digital signature algorithm (ECDSA) in DNSSEC, IEEE-2017, DOI: 10.1109/CNSM.2016.7818428.
- [28] Roland van Rijswijk-Deij, Anna Sperotto and Aiko Pras, Making the case for elliptic curves in DNSSEC, ACM SIGCOMM Computer Communication Review archive Volume 45 Issue 5, October 2015, DOI:10.1145/2831347.2831350.
- [29] Matthäus Wander, "Measurement survey of server-side DNSSEC adoption", IEEE-2017, DOI: 10.23919/TMA.2017.8002913.
- [30] Tanmay Chattergee, Configuration of DNS server with cryptographic algorithm for secure DNS and DHCP updates, IEEE-2012, DOI: 10.1109/ICCCNT.2012.6395990. Roland van Rijswijk-Deij, Mattijs Jonker and Anna Sperotto, On the adoption of the elliptic curve digital signature algorithm (ECDSA) in DNSSEC, IEEE-2017, DOI: 10.1109/CNSM.2016.7818428.
- [31] Naveen Kumar Tiwari and Sanjay Khakhil, Security system for DNS using cryptography, International Journal of Computer Applications (0975-8887), Volume 120 – No. 17, June 2015.
- [32] Preeti Thareja and Mrs. Neeru Arora, Securing DNS using ECC, IEEE-2014, and Electronic ISBN: 978-1-4799-4236-7, DOI: 10.1109/CONFLUENCE.2014.6949246.
- [33] Naveen Kumar and Kamal Kumar Ranga, A framework for security of DNS using cryptography, IJIRST-International Journal for Innovative Research in Science & Technology, Volume 2, Issue 01, June 2015, ISSN (Online) : 2349-6010.
- [34] Roland van Rijswijk-Deij, Kaspar Hageman and Anna Sperotto, The performance impact of elliptic curve cryptography on DNSSEC validation, IEEE-2016, DOI: 10.1109/TNET.2016.2605767.

Authors Biography

¹Ms. Maitri Patel

Ms. Maitri Patel is a Ph.D Scholar in Computer Engineering Department of Sankalchand Patel College of Engineering, Visnagar. She completed her B.E. in Computer Engineering from Gujarat University and M.Tech in Computer Science and Engineering from Jodhpur University. She published and presented research articles in International/National level of Conferences and Journals. Chaired a technical session for two days international conference



on “ICT for Sustainable Development” Organized jointly by ASSOCHAM (India-Gujarat Chapter), GESIA, and ACM Chapter.

²Dr. Rajan Patel

Dr. Rajan Patel is an Associate Professor in Computer Engineering Department of Sankalchand Patel College of Engineering, Visnagar. Dr. Patel has more than 11 professional memberships. He completed his B.E. in Computer Engineering from Saurashtra University and M.Tech in Computer Engineering from NIT, Surat. He did his Ph.D. in Computer Engineering in the domain of MANET Security from RK University. Dr. Patel published and presented research and survey articles in International/National level of indexing Conferences and Journals including IEEE, Science Direct, Springer, Elsevier. Dr. Patel received more than 11 Award/Honored/Excellence/Appreciation from academic bodies such as Certificate of Excellence as a coordinator for conduction of sponsored ICT (MHRD) two-week ISTE workshop from IIT, Bombay in 2014, Appreciation from the Dewang Mehta Innovation IT award in 2015, Honored in the Technical Communication workshop from IIT-Bombay in 2015, Paper Presenter Award at International Conference by CSI in 2017. Dr. Patel coordinated and organized many STTPs/Seminars/Talks and also having the participation of more than 39 Conferences/STTPs/Seminar/Workshop. Dr. Patel is acted as a Reviewer/TPC member of IEEE, Springer and other International/National conferences and IET Network Journal. Dr. Patel also worked for ISEAP sponsored MHRD project during his Post graduation period at NIT, Surat.



