UNIVERSITI PUTRA MALAYSIA

PROTECTING DNS FROM REFLECTION AMPLIFICATION ATTACKS USING DISTRIBUTED DEFENSE SCHEME

DANA HASAN AHMED

FSKTM 2018 4

PROTECTING DNS FROM REFLECTION AMPLIFICATION ATTACKS USING DISTRIBUTED DEFENSE SCHEME

By

DANA HASAN AHMED

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

November 2017

DEDICATION

I would like to dedicate this work to those who taught, motivated and helped me throughout my study.

To my beloved parent, sibling, and friends

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

PROTECTING DNS FROM REFLECTION AMPLIFICATION ATTACKS USING DISTRIBUTED DEFENSE SCHEME

By

DANA HASAN AHMED

November 2017

Chairman : Masnida Hussin, PhD
Faculty : Computer Science and Information Technology

Domain Name System (DNS) is based-on distributed, hierarchical, client-server architecture that translates domain names into Internet Protocol (IP) addresses and vice versa. It relies on User Datagram Protocol (UDP) to transport its data and uses IP in the network layer protocol. Normally, DNS receives requests from its source and sends back the substantially larger responses without inspecting the source address. Lack of source inspection is due to the fact that UDP is a connectionless protocol and IP address does not provide authentication mechanism. Furthermore, DNS is designed for naming efficiency, not security. Such scenarios make DNS a tempting target for cybercriminals to perform massive Distributed Reflection Denial of Service (DRDoS) attacks which are called Reflection/Amplification and hassles the communication traffic towards connected network nodes. There are several defense mechanisms that proposed to tackle DNS Reflection/Amplification attack. They depend on centralized-based approaches where their functionalities degrade against large and complex traffic. In this research, Distributed-based Defense Scheme (DDS) is proposed to monitor incoming DNS requests for handling DNS Reflection/Amplification attacks and a filtration mechanism to distinguish legitimate requests from fake ones. It utilizes an authentication mechanism called DNS Checkpoint which is based on Challenge-Handshake Authentication Protocol (CHAP) to provide authentication for detecting any Reflection/Amplification attacks. The DNS Disinfector is used for filtering mechanism that based-on Stateful Packet Inspection (SPI). It is used to distinguish legitimate requests and discard the fake ones. The experiment results show that DDS remarkably overcome the single-point deployment defense mechanism in terms of defense strength, minimizing amplification factor and less bandwidth usage. The results analysis also shows that DDS able to better protect upstream networks from depletion than other defense mechanisms with minimum overhead.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

MELINDUNGI DNS DARIPADA SERANGAN PANTULAN/PENGUATAN MELALUI SKIMA PERTAHANAN TERAGIH

Oleh

DANA HASAN AHMED

November 2017

Pengerusi : Masnida Hussin, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Sistem Nama Domain (DNS) ialah berasaskan seni bina teragih, hierarki dan senibina pelanggan-pelayan yang menterjemah nama domain kepada alamat Protokol Internet (IP) dan juga sebaliknya. Ia bergantung kepada Protokol Datagram Pengguna (UDP) untuk menghantar data dan menggunakan IP sebagai protokol pada lapisan rangkaian. Lazimnya, DNS menerima permintaan daripada sumber dan menghantar kembali respons yang lebih besar tanpa memeriksa alamat sumber. Ketiadaan pemeriksaan sumber ialah kerana UDP merupakan protokol tanpa sambungan dan alamat IP tidak menyediakan mekanisme pengesahihan. Tambahan pula, DNS direka untuk penterjenamahan nama dan bukan untuk keselamatan. Senario ini menjadikan DNS sebagai sasaran penjenayah siber bagi melakukan serangan Nafi Khidmat Pantulan Teragih (DRDoS) yang dikenali sebagai pantulan/amplifikasi dan mengganggu trafik komunikasi pada nod rangkaian yang bersambungan. Terdapat beberapa mekanisme pertahanan yang dicadangkan untuk menangani serangan pantulan/amplifikasi DNS. Mekanisme-mekanisme tersebut menggunakan pendekatan berpusat yang menyebabkan kemampuan fungsi keselamatan terjejas terutama bagi trafik yang kompleks dan besar. Di dalam penyelidikan ini, mekanisme pertahanan teragih yang dinamakan sebagai Skim Pertahanan Teragih (DDS) telah dicadangkan untuk mengawal permintaan masuk DNS bagi menghadapi serangan pantulan/amplifikasi DNS serta mekanisme penapisan untuk membezakan di antara permintaan yang sah dan palsu. Ia menggunakan mekanisme pengesahihan Titik Semakan DNS yang berdasarkan Protokol Pengesahan Jabat Tangan Cabar (CHAP) bagi mengesan serangan pantulan/amplifikasi. Teknik Penyahjangkit DNS pula berperanan sebagai mekanisme penapisan yang berasaskan Pemeriksaan Paket *Stateful* (SPI). Ia bertujuan bagi menentukan permintaan sah dan menolak permintaan palsu. Hasil daripada proses simulasi mendapati bahawa DDS mampu memberi prestasi yang lebih baik berbanding dengan mekanisme pertahanan berpusat terutamanya daripada

segi kekuatan pertahanan, pengurangan faktor amplifikasi dan penggunaan jalur lebar. Hasil analisa keputusan juga menunjukkan DDS mampu melindungi rangkaian dengan lebih baik berbanding mekanisme pertahanan yang lain dengan minima overhed.

ACKNOWLEDGEMENTS

All praises are for Allah, the most gracious, the most merciful who taught human with means of pen how to write and taught man which he knew not.

I would like to express my heartfelt appreciation to Dr Masnida Hussin, the chairman of my supervisory committee for his advice and guidance, tolerance and encouragements, fruitful criticism, close supervision and patience in reading this dissertation and my manuscript thoroughly in a short time. She offered me an opportunity for the improvement of my scientific knowledge and research work. Moreover, she made available all the research materials timely to enable me complete the research work smoothly and on time, so I cannot thank her enough for her contribution to my understanding of research.

I would like to gratefully acknowledge the effort of Dr Azizol Abdullah, my supervisory committee member for his valuable advice, guidance and scholarly criticism throughout my study time. I thank him for the role he played towards the successful completion of my research.

I would like to express my heartfelt thanks to my beloved parents, brothers and sisters who in one way or the other made my dreams to achieve this degree, and their constant prayers and encouragements to accomplish my goals. Allah may continue to reward you abundantly.

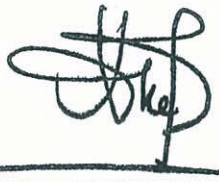
I certify that a Thesis Examination Committee has met on 17 November 2017 to conduct the final examination of Dana Hasan Ahmed on his thesis entitled "Protecting DNS from Reflection Amplification Attacks using Distributed Defense Scheme" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Rohaya binti Latip, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Amir Rizaan bin Abdul Rahiman, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Shukor Abd Razak, PhD
Associate Professor
Universiti Teknologi Malaysia
Malaysia
(External Examiner)



NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 29 January 2018

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Masnida Hussin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby declare that:

- this thesis is based on my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual properties from the thesis and copyright of thesis are fully owned by the Universiti Putra Malaysia, as according to the Universiti Malaysia (Research) rule 2012;
- written permission must be obtained from the supervisor and the office of the deputy Vice Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journal, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis and scholarly integrity is upheld as according to the University Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the University Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Dana Hasan Ahmed ,GS43221

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and writing of this thesis was under our supervision,
- supervision responsibilities as stated in Rule 41 in Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Dr. Masnida Hussin

Signature: _____
Name of Member of Supervisory Committee: Dr. Azizol Abdullah

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

LIST OF ABBREVIATIONS

A	A record
AAAA	Quad-A record
AaaS	Authentication as a Service
ANS	Authoritative Name Server
AS	Autonomous System
CCN	Content-Centric Networking
CPU	Central Processing Unit
DAAD	DNS Amplification Attack Detector
DDAA	Detecting DNS Amplification Attack
DDoS	Distributed Denial of Service
DDS	Distributed Defense Scheme
DNS	Domain Name System
DNSKEY	DNS Key record
DNSSEC	DNS Security Extension
DoS	Denial of Service
DRDoS	Distributed Reflective Denial of Service
FN	False Negative
FP	False Positive
FQDN	Fully Qualified Domain Name
Gbps	Gigabit per Second
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
JDBC	Java Database Connectivity
JPCAP	Java Packet Capture
LRS	Local Recursive Server
MX	Message Exchange record

NS	Name Server record
NTP	Network Time Protocol
ODBC	Open Database Connectivity
OSI	Open System Interconnection
OTP	One-Time Password
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comments
RR	Resource Record
RRL	Response Rate Limiting
RRSIG	Resource Record Signature
Sec	Second
SOA	Start of Authority
SPI	Stateful Packet Inspection
Tbps	Terabit per second
TCP	Transport Control Protocol
TLD	Top Level Domain
TN	True Negative
TP	True Positive
TTL	Time to Live
TXT	Text
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

1.1 Background and motivation

Domain Name Service (DNS), if not the most critical, is a crucial element of Internet infrastructure (Anagnostopoulos, Kambourakis, Kopanos, Louloudakis, & Gritzalis, 2013). It is a distributed, hierarchical naming system for the resources connected to the Internet (i.e. computer, servers, and services). DNS allows organization of various information elements with allotted domain names. It translates human-readable domain names into computer-readable Internet Protocol (IP) addresses and vice versa. Given over 30 years from its development, DNS is successfully matured into an essential part of the Internet today. Any unavailability in this service, causes huge inconvenience on the global scale (Rossow & Horst, 2014). As announced by Web Server Survey which is operated by Netcraft, the number of reserved web domains are over 1.8 billion. They may not be active websites. However, their domains are parked or something comparable (Netcraft, 2017).

The DNS was initially designed when the internet protocols were defined with no security concerns. It mostly takes advantage of User Datagram Protocol (UDP) as transport layer protocol, which is a connectionless protocol with no handshaking - connection establishment mechanisms. Also, it utilizes IP as network layer protocol, as such with no provision for source authentication mechanism. DNS responses larger than the corresponding requests, by a ratio called amplification factor. And, when a DNS server receives a request, it sends back responses without knowing the identity of the requesting source indicated by the packet.

The awareness of these vulnerabilities in the DNS made it possible for cybercriminals to, with a little effort, fabricate malware that utilizes the DNS as an environment to penetrate into both the sever and its clients and perform unauthorized or malicious activities (Marrison, 2014). These facts make the DNS infrastructure as a soft target for malware and cybercrimes, by considering the DNS infrastructure coordinates the core services on the Internet (i.e. www, email). As reported by (Woolf, 2016), when a DNS server is down, its operation domain become unavailable too, increasing the likelihood of wide-scale disturbances. The discovery of the security threats associated with these DNS vulnerabilities, in the last few years, draws the attention of cyber security community to re-consider its design. One of the most usual and nasty types of threats is Reflection/Amplification attacks, for which to counter is very costly (Di Paola & Lombardo, 2011). It is a cyber-attack which falls under Distributed Denial of Service (DDoS) attack category. This attack can be initiated by fabricating a spoofed datagram with target's IP address by the attacker. The attacker sends the datagram to a DNS server which in its turn send the

response back to the victim. The reflection of the DNS response occurring because the request datagram has spoofed header and the DNS server cannot differentiate spoofed addresses from legitimate ones. The process generates unsolicited traffic in the victim's machine and thus unnecessarily consumes its resources. The easiness of the DNS Reflection/Amplification attack results from the fact that IP provides no source authentication mechanism to countermeasure the attack; this is coupled with the fact that UDP is connectionless, that uses no handshaking mechanism. Therefore, it is very easy for the attacker to forge the victim's address and send to the DNS servers a datagram containing the address, and the DNS unknowingly reflected it to the victim. The victim is left helplessly engaged in responding to the server to protect its bandwidth and processing resources from further being wasted by the unsolicited datagram. Thus, consequent to the UDP's absence of connection establishment through a handshake and the lack of source authentication, the DNS become a handy tool for amplification attack that results in massively flooding the victim's resource with DDoS.

Recently, attackers succeed in generating hundreds to thousands of Gbps DDoS traffic through the attack. An example is an attack on DYN company that occurs on October, 21st 2016 which reached the peak of 1.2 Terabit per second (Tbps). DYN controls many domain names on the Internet (Rossow & Horst, 2014) (Woolf, 2016). The attack disrupted the Internet for several days, and renders popular websites such as Amazon and Twitter helplessly unavailable during the period. Most of the current-operating defense mechanisms fail to mitigate an attack with such a magnitude. What makes the matter worse, the attacker could continuously change the reflection servers traffic rate and other parameters (i.e. such as port and resource records) to hugely increase the attack complexity and avert any defense mechanism and prevent countering the flow of their attack (Di Paola & Lombardo, 2011).

There required three steps for any defense system against such attack: first, accurately detect these attacks; then timely respond by stopping the incoming flooding attack traffic; and it is equally necessary to differentiate a legitimate traffic that shares the same signature with that of the attack and delivers it without failing the victim. Unfortunately, there is yet to be any single point of defense mechanism that meets all the three requirements: The attack detection is most accurately possible at the victim side while response is mostly successful close to attacking source (Wang et al., 2014) (Zargar, Joshi & Tipper, 2013). Due to the fact that the DNS amplification attack is a distributed by its nature, a distributed defense mechanism is required to counter it from multiple nodes. Most of the current defense mechanisms are centralized, for which the protection capacity is easily degraded with increasing magnitude, and complexity of the attack. This is as recent incidents revealed (Zargar et al., 2013) (Woolf, 2016). In this research, we proposed Distributed Defense Scheme (DDS) to counter the DNS DDoS attacks (i.e. Reflection/Amplification attacks). This is due to our observing that an optimal strategy is to have a defense mechanism deployed from multiple nodes, so that more resources are pooled for the protection with even better detection accuracy. Also, the strategy is

aimed at protecting the upstream victim networks from exhaustion as the result of the attack magnitude.

1.2 Problem statement

DNS utilizes UDP as transport layer for most of its transactions for smooth and better performance in Internet naming system. Thus, it demands no handshaking or connection establishment due to the connectionless protocol. Furthermore, only one packet is utilized in the name resolution request to the DNS, and most of the times it responses by the DNS with one response packet, which leads to source authentication problem (Anagnostopoulos et al., 2013). Though the authors in (Herzberg & Shulman, 2014) proposed the mechanism so-called Authentication as a Service (AaaS) for the DNS, it is only limited to Cloud-based networks and, thus, cannot protect the structure of the Internet. Basically, the DNS response packet sizes are larger than the corresponding request. This makes the DNS a "good" attack medium for amplifying the size of the attack traffic. One of the cyber-attack that related to DNS is Reflection/Amplification attacks (Douglas C. MacFarland, Craig A. Shue, 2015). This kind of cyber threat can disrupt any network from upstream to the attack's victim if it has sufficient strength. Currently, most of the defense mechanisms are utilized the centralized-based defense strategy that could not fully protects networks at both upstream and downstream connections. The centralized defense mechanisms are lack of strength to defend against DNS Reflection/Amplification attacks. Also, they have shortcomings in identification and separation of legitimate and bogus traffics. It is because they are non-holistic defense strategies. This weakness leads to getting false outcome in detecting threats in network traffic. In order to protect networks from such threat, a distributed-based defense mechanism is required. This study proposed the defense mechanism based on distributed infrastructure where it should be deployed from multiple nodes. The nodes are cooperated to protect the network traffic and path from becoming victim and being flooded with DNS responses (Zargar et al., 2013) (Mirkovic, Robinson, Reiher, & Oikonomou, 2005).

From these facts, we identify two specific problems in DNS as related to its current defense mechanism against amplification attack as follows.

i. By default, DNS amplifies every response to each request thereby making the amplification attack become easier to deploy. With few reflections, it floods the victim's bandwidth with bogus traffic. While finding necessary solutions; to the best of our knowledge, there was no other researches that attempt to reduce the impact of the DNS amplification in distributed infrastructure while maintaining the Quality of Service (QoS) in the DNS.

ii. The identification and separation between legitimate and bogus traffics is significance solution in DNS. However, current filtration mechanisms cannot fully separate legitimate traffic from the spoofed one. Moreover, the

ability to filter the traffic based on the traffic flow is difficult to handle due to DNS utilized UDP protocols, and even though it is able to filter it gives false outcome. There are other researchers' focuses on the filtration based on packet inspection, however it is inefficient, time consuming and not practical in dynamic and heterogeneous environment like DNS. Therefore, we need filtration strategy to be executed in effective way to differentiate both legitimate and bogus traffics in DNS.

1.3 Research objectives

This study is carried out with the aim of tackling DNS Reflection/Amplification attack using distributed-based defense mechanism. The specific objectives of this study are

i. To propose an authentication scheme between authoritative name servers and the victim's server in distributed infrastructure in order to prevent spoofed-DNS response while reducing the impact of DNS amplification.
ii. To propose a filtration strategy based on the outcome of the authentication scheme to separate the legitimate traffic from fake one. It then discarded the spoofed traffic flaw to ensure optimal detection accuracy with acceptable efficiency.

1.4 Research scope

This research falls under the category of IP spoofing detection, at the intermediate-destination networks. The detection mechanism is proposed to take place at network and transport layer of Open System Interconnection (OSI) model of the network. We focused on distributed filtering strategy to achieve optimal detection accuracy, efficiency and mitigating the impact, to the lowest possible on the upstream networks, of amplification factor during Reflection/Amplification attacks. We intend to show how the distributed defense mechanisms can better protect networks than centralized ones.

This research focused on the authentication of DNS transactions (request and response), alongside with filtering of spoofed requests. Other details about the DNS request, response, and type of queries are not considered. Three activities are simulated in the research: Distributed Defense Scheme (DDS), Detecting DNS Amplification Attack (DDAA), and Response Rate Limiting (RRL). All lost packets in experiments are ignored to clarify how these experiments operate against Reflection/Amplification attacks in DNS, in a controlled computational-environment condition.

1.5 Thesis organization

This thesis is organized into five chapters as follows.

In Chapter one, the background of the study is established. We also stated our motivation for the research, as well as the research problems and objectives to be achieved. The Chapter also detailed the scope and limitation of this research.

The following Chapter begins with a background on the DNS and its vulnerability that makes the Reflection/Amplification attacks possible. The related literature is also critically reviewed. The Chapter is finally concluded with limitations of the fast works to address the identified problem which we proposed to address.

Chapter three discussed the general the methodology adopted in this research in, among others, classifying DNS request packets to ensure their legitimacy. The chapter explains detail the system model and its operations when fully functional. Also the authentication mechanism and filtration mechanism are developed in detail. The hardware and software tools utilized to design the experiment and its environment are discussed. And the formulation of attack and its scenarios are explained. On top of that, all related metrics are discussed in detail

Chapter four is about running the experiments, collecting output data of the systems, and drawing the results from those data based on related metrics in chapter 3. We run our authentication mechanism side-by-side with our filtration strategy to achieve optimal detection results with minimum false outcomes.

In Chapter five, we conclude the research and recommend on possible future enhancements of this work.

REFERENCES

Abbasi, S. (2014). *Investigation of Open Resolvers in DNS Reflection DDoS Attacks* (Doctoral dissertation, Université Laval).

Aitchison, R. (2011). *Pro Dns and BIND 10*. Apress.

Akami Technologies. (2014). *Domain Name System (DNS) Flooder Threat Advisory*. Retrieved from https://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-dns-flooder.html

Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., & Gritzalis, S. (2013). DNS amplification attack revisited. *Computers & Security*, *39*, 475-485.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Arbor Networks, (2017). *12thannual Worldwide Infrastructure Security Report*. Retrived from http://email.arbornetworks.com/VGNX000lIm0A000KZfd0Zl0

Baker, F., & Savola, P. Ingress filtering for multi home networks IETF RFC 3704, MAR 2004.

Benton, K., Camp, L. J., Kelley, T., & Swany, M. (2015, September). Filtering ip source spoofing using feasible path reverse path forwarding with sdn. In *Communications and Network Security (CNS), 2015 IEEE Conference on* (pp. 733-734). IEEE.

Bisiaux, J. Y. (2014). DNS threats and mitigation strategies. *Network Security*, *2014*(7), 5-9.

Cisco Systems, I. (2014). *Cisco Prime Network Registrar* (8.2 ed.). Retrieved from http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_registrar/8-2/user/guide/CPNR_8_2_User_Guide.pdf

Di Paola, S., & Lombardo, D. (2011, July). Protecting against DNS reflection attacks with Bloom filters. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 1-16). Springer Berlin Heidelberg.

Dordal, P. L. (2017). An introduction to computer networks.

Ferguson, P., & Senie, D. RFC-2827 "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", 2000. *See*

also BCP0038. Obsoletes RFC2267. Status: BEST CURRENT PRACTICE.

Gibbs, P. M. (2014). *Botnet Tracking Tools*. Retrived from https://www.sans.org/reading-room/whitepapers/detection/botnet-tracking-tools-35347

Herzberg, A., & Shulman, H. (2014, December). DNS authentication as a service: preventing amplification attacks. In *Proceedings of the 30th Annual Computer Security Applications Conference* (pp. 356-365). ACM.

Huawi. (2014). *2014 Botnets and DDoS Attacks Report*. Retrieved from http://e.huawei.com/en/marketing-material/global/products/enterprise_network/security/anti-ddos/hw_315881

Inamura, M. (2015, February). Expansions of CHAP: Modificationless on its structures of packet and data exchange. In *Information Systems Security and Privacy (ICISSP), 2015 International Conference on* (pp. 1-8). IEEE.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009, December). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies* (pp. 1-12). ACM.

Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2008). Detecting DNS amplification attacks. In *International Workshop on Critical Information Infrastructures Security* (pp. 185-196). Springer Berlin Heidelberg.

Kaminsky, D. (2008). Multiple dns implementations vulnerable to cache poisoning. *US Computer Emergency Readiness Team, Tech. Rep*, *800113*.

Koç, Y., Jamakovic, A., & Gijsen, B. (2012). A global reference model of the domain name system. *International Journal of Critical Infrastructure Protection*, *5*(3), 108-117.

Kührer, M., Hupperich, T., Rossow, C., & Holz, T. (2014, August). Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks. In *WOOT*.

Kührer, M., Hupperich, T., Rossow, C., & Holz, T. (2014). Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *USENIX Security* (Vol. 2014).

Kurose, J. F., & Ross, K. W. (2016). Computer Networking A Top Down Approach Featuring The Intel.

Lavanya, M., & Sahoo, P. K. (2016). IP spoofing and its Detection Technique. *IJACTA*, *4*(1), 167-169.

Liu, B., Li, J., Wei, T., Berg, S., Ye, J., Li, C., ... & Han, X. (2015). SF-DRDoS: The store-and-flood distributed reflective denial of service attack. *Computer Communications*, *69*, 107-115.

MacFarland, D. C., Shue, C. A., & Kalafut, A. J. (2015, March). Characterizing optimal DNS amplification attacks and effective mitigation. In *International Conference on Passive and Active Network Measurement* (pp. 15-27). Springer International Publishing.

Majkowski, M. (2015). Deprecating the DNS ANY meta-query type. Retrived from https://blog.cloudflare.com/deprecating-dns-any-meta-query-type/

Marrison, C. (2014). DNS as an attack vector–and how businesses can keep it secure. *Network Security*, *2014*(6), 17-20.

Mirkovic, J., Robinson, M., Reiher, P., & Oikonomou, G. (2005). Distributed defense against DDOS attacks. *University of Delaware CIS Department technical report CIS-TR-2005-02*, 1-12.

Miyata, H. (2015). *A study on real-time communications management based on packet propagation time monitoring and hop-by-hop packet authentication for process automation* (Doctoral dissertation, 東京農工大学).

Musashi, Y., Takeda, Y., Shibata, N., Kautsar, I. A., & Sugitani, K. (2013). A statistical study of ANY resource record based DNS query request packet traffic. *Information (Japan)*, *16*(12 B), 8901-8908.

Netcraft (2017). *Web Server Survey*. Retrived from http://www.internetlivestats.com/total-number-of-websites/

Paluskar, Y. S., Agarwal, P. M., Tambe, R. R., & Agarwal, S. N. (2013). Controlling IP spoofing through inter domain packet filters. *International Journal of Students' Research in Technology & Management*, *1*(3), 347-352.

Ploskas, N., Stiakakis, E., & Fouliras, P. (2015). Assessing Computer Network Efficiency Using Data Envelopment Analysis and Multicriteria Decision Analysis Techniques. *Journal of Multi‐Criteria Decision Analysis*, *22*(5-6), 260-278.

Powers, D.M.W., 2011. Evaluation: from Precision, Recall and F-measure to ROC, Informedness, Markedness and Correlation. *Journal of Machine Learning Technologies*, 2,(1), 37-63.

Rafiee, H., von Löwis, M., & Meinel, C. (2013). Challenges and Solutions for DNS Security in IPv6. *Architectures and Protocols for Secure Information Technology Infrastructures*, 160.

Ronald van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2014, November). DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 449-460). ACM.

Rossow, C. (2014, February). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *NDSS*.

Rozekrans, T., Mekking, M., & de Koning, J. (2013). *Defending against DNS reflection amplification attacks*. University of Amsterdam.

Ryba, F. J., Orlinski, M., Wählisch, M., Rossow, C., & Schmidt, T. C. (2015). Amplification and DRDoS Attack Defense--A Survey and New Perspectives. *arXiv preprint arXiv:1505.07892*.

Singh, S. P. (2012). The Use of DNS Resource Records. *International Journal of Advances in Electrical and Electronics Engineering (IJAEEE, ISSN: 2319-1112)*, *1*(02), 230-236.

Turner, D. M. (2016). D*igital authentication - The basics*. Retrieved from https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics

Vixie, P., & Schryver, V. (2012). Dns response rate limiting (dns rrl). *URL: http://ss. vix. su/~ vixie/isc-tn-2012-1. txt*.

Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., & Stavrou, A. (2014). A moving target DDoS defense mechanism. *Computer Communications*, *46*, 10-21.

Woolf, N. (2016). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. Retrived from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Ye, X., & Ye, Y. (2013). A practical mechanism to counteract DNS amplification DDoS attacks. *Journal of Computational Information Systems*, *9*(1), 265-272.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, *15*(4), 2046-2069.