社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

DNSのセキュリティ問題の現在と未来

力武　健次†　　鈴木　常彦††,†††中尾　康二†,††††

† 情報通信研究機構 インシデント対策グループ　〒184–8795 東京都小金井市貫井北町 4–2–1
†† 中京大学 情報理工学部　〒470–0393 愛知県豊田市貝津町床立 101
††† 株式会社リフレクション　〒460–0008 愛知県名古屋市中区栄 3-1-26
†††† KDDI 株式会社　〒102–0072 東京都千代田区飯田橋 3–10–10
E-mail: †rikitake@nict.go.jp

あらまし　ドメイン名システム (DNS) はドメイン名と IP アドレスなど各種の資源を対応付けるのに必要不可欠なインターネット上のサブシステムである．しかし，DNS の仕様は文書で形式的に決められたものではなく，運用者は動作している実装のふるまいからシステムの大半を学ぶ必要がある．同様に運用者は DNS プログラムの相互接続性を維持するために，実装に依存する問題の詳細にわたって理解する高度な経験を持つ必要がある．このような経験に依存する運用は DNS を脆弱かつセキュリティ攻撃に対し弱いものにしている．本稿では，新たに起こりつつある DNS のセキュリティ問題について運用の立場から分析し，それらの解決のために取り得る手段について示す．
キーワード　DNS（ドメイン名システム），ネットワーク運用，セキュリティ脅威分析，ドメイン管理

DNS Security: Now and The Future

Kenji RIKITAKE†, Tsunehiko SUZUKI††,†††, and Koji NAKAO†,††††

† Network Security Incident Response Group, NICT, Japan
4-2-1, Nukui-Kitamachi, Koganei City, Tokyo 184-8795 Japan
†† School of Information Science and Technology, Chukyo University
101, Tokodachi, Kaizu-cho, Toyota City, Aichi 567-0047 Japan
††† Reflection Co., Ltd.　3-1-26, Sakae, Naka-ku, Nagoya City, Aichi 460-0008 Japan
†††† KDDI Corporation　3-10-10, Iidabashi, Chiyoda-Ku, Tokyo 102-0072 Japan
E-mail: †rikitake@nict.go.jp

Abstract　Domain Name System (DNS) is an essential Internet subsystem for binding domain names and various resources including IP addresses. The specification of DNS, however, is not formally defined on documentations, and the operators have to learn the system mostly from the behavior of running implementations. The operators also have to have a high level of expertise to understand the implementation-dependent issues in details for maintaining the interoperability of DNS programs. This expertise-dependent operation makes DNS fragile and prone to security attacks. In this paper, we analyze the emerging DNS security issues from the operational points of view, and show possible countermeasures to solve the issues.
Keywords　DNS (Domain Name System), network operation, security threat analysis, domain name management

1. Introduction

Domain Name System (DNS) [1]〜[3] is an essential Internet distributed database subsystem to map domain names to various Resource Records (RRs). Web, e-mail, and many other applications depend on DNS for discovering the destination hosts to contact. Keeping the DNS up-to-date and secure without forgery or service disruption is critical for providing the reliable services on Internet.

DNS has been widely used for mapping domain names to IPv4 addresses and vice versa. Mail exchanger host reference using MX RRs is another popular usage. More applications assume registering crucial information on DNS. DomainKeys Identified Mail (DKIM) [4] and Sender Policy Framework (SPF) [5] are two major proposals for identifying mail senders with the corresponding TXT and SPF RRs.

Public information for cryptographic communication is also being registered into DNS, such as those to put Secure Shell [6] fingerprints to SSHFP RRs [7], IPsec [8] public keys to IPSECKEY RRs [9], and X.509 certificates and the revocation lists to CERT RRs [10].

Identification for available resources to a service name is another popular usage of DNS, such as binding service names to actual hosts by SRV RRs [11], and binding a telephone number as a part of E.164 number to the available services [12] with NAPTR RRs, which are defined in Dynamic Delegation Discovery System [13]〜[16].

Dynamic Host Configuration Protocol (DHCP) [17], [18] and the resolution scheme of domain name conflicts of the clients [19]〜[21] uses the DHCID RR [22] to uniquely identify the clients, for the accurate dynamic update of DNS using DNS UPDATE [23] protocol.

The examples shown above suggest a convergence of domain-name-related resource database into DNS. However, the *traditional DNS*, which stands for the current DNS system without cryptographic authentication, is considered one of the weakest subsystems on Internet, as well as the IP routing protocols. The following is a list of well-known weaknesses of DNS:

- The traditional DNS handles only 512 bytes on the UDP payload for a message, which imposes the limit of containing multiple addresses, especially when IPv4 and IPv6 addresses have to be assigned together.
- The DNS database integrity is solely dependent on a weak authentication by maintaining the delegation tree from the Root Zone to the subzones only with the NS RRs, with no protection of cryptographic signatures.
- DNS RR data are historically configured by the zone operators/administrators, so the contents are prone to human errors.

Among the Internet RFCs, Klensin [24] discusses the role and the overloaded status of DNS, while Atkins and Austein [25] thoroughly analyze the threats of DNS.

Two notable extensions are proposed for the authentication of DNS. DNSSEC [26]〜[28], a cryptographic authentication scheme for DNS RRs, has been proposed and is under deployment phase. EDNS0 [29] is another extension which allows larger payloads over DNS UDP datagrams. Those extensions alone, however, will not sufficiently solve the whole security issues persistently hamper the DNS reliability and integrity.

In this paper, we survey and analyze the current and emerging issues on DNS security from the operational points of view, and show the possible countermeasures to solve them. In later sections, we first analyze the security issues on emerging new DNS protocols in Section 2, and survey the persistence of long-term problems and issues of DNS operation in Section 3. We conclude this paper by showing the conclusions and possible countermeasures to solve the current DNS issues in Section 4.

2. DNS security and emerging protocols

2.1. IPv6 and DNS

Introduction of IPv6 is being discovered as a serious issue to maintain the DNS reachability and integrity. The AAAA RR and `ip6.arpa` are two new RRs assigned for IPv6 [30], but the problem is not limited to them.

The AAAA RRs will increase the size of DNS answers and will reduce the number of the NS RRs, especially for those with IPv4 *and* IPv6 glue addresses [*1] . The current limit of 13 Root Servers is imposed by the 512-byte size limit of the DNS answers, and the limitation gets even tighter when IPv6 is fully introduced. This issue will not be solved unless the full support of EDNS0 on *all* DNS clients, servers, and the intermediate firewalls. Internet Corporation for Assigned Names and Numbers (ICANN) recognizes the importance of this issue, and their report [31] shows not all devices are compatible with larger-than-512-byte packets. Rikitake [32] shows a comprehensive analysis on this issue.

IPv6 also introduces another requirement for all DNS servers to make them accessible in both networks of IPv4 *and* IPv6. This means querying IPv4 data from IPv6 and vice versa must be possible, and the DNS database must be fully consistent regardless of the access path. Even during the *transition* [*2] phase from IPv4 to IPv6, the DNS has to be operational on both networks. Unless all the IPv4 hosts are eliminated from the Internet, which will not be likely to happen, DNS has to serve for the two networks forever. For DNS, supporting IPv6 is not a *transition*, but a complete *addition* of a new functionality set.

The reality of operational networks as of August 2007 is far from the requirement of dual-stack operation of DNS over IPv4 and IPv6. Very few authoritative servers are accessible from the IPv6 network. Many IPv6 experimental networks have an workaround to this issue by providing and IPv6 DNS cache to get access to IPv4 DNS servers, though very few networks provide an IPv4-to-IPv6 DNS lookup service.

Another issue is that NS RRs only show hostnames and do not directly represent if the host specified is accessible

*1 : The *glue* addresses are the address records (A and AAAA RRs) attached to an NS RR, so that the server referred by the NS RR is accessible without sending another query.

*2 : as claimed in RFC4213 [33] since the officialization of IPv6 in 1994 by IETF and IAB. RFC4213 suggests the DNS requirement in the Section 2.2.

via IPv4 or IPv6. While a preference-based address resolution is proposed for an IP-level choice [34], the preference for DNS lookups should be based on the actual information obtained from the servers. A DNS server lookup will require two lookups for AAAA and A RRs, instead of one.

The requirement of simultaneously looking up IPv4 and IPv6 DNS servers may cause a delay on DNS lookup in many situations. For example, even if a DNS server on an NS RR is accessible via IPv4, if the resolver chooses DNS lookup on IPv6 as the first choice for the server, the lookup will fail, and the resolution delays until the resolver performs the second try on IPv4. Morishita and Jinmei [35] describe some common misbehaviors of DNS servers to the queries for IPv6 addresses. WIDE Project [36] has released a report of measuring the performance difference between the IPv4 and IPv6 networks by comparing delay measurements using dual-stack nodes [37]. A similar measurement should be performed for the DNS services by the providers.

2. 2. DNSSEC deployment issues

IETF dnsext WG [38] did not have the WG meeting at the 69th IETF on July 2007, since most of the WG milestones including DNSSEC standardization of the fundamental protocols were completed. This WG decision suggests that the DNSSEC developing community has reached to a consensus that DNSSEC is now on the deployment phase.

DNSSEC Deployment Initiative, a coordination community of DNSSEC developers and other interested parties, publishes a monthly newsletter called *DNSSEC This Month* [39]. The Initiative focuses on how to deploy the existing DNSSEC technologies to various DNS registries and other organizations. Some notable progressive actions are:

- The status of signed zones of `.arpa` and the Root Zone is available online by IANA [40], though still experimental as of August 2007.
- RIPE NCC, representing the European concerns of DNSSEC, formally requested ICANN to sign DNS Root Zone [41], as a community-endorsed resolution at the RIPE 54 meeting on May 2007.

Some protocol issues of DNSSEC still remain, however, such as whether to introduce the NSEC3 RR [42] instead of NSEC RR for defending a zone from an exploit by enumaration. The current DNSSEC specification does not define the formal zone revocation method either [*3] .

3. Persistent operational issues

3. 1. Lame and inconsistent zone delegation

Lame delegation [*4] has been a persistent problem on DNS operation. Many of them are caused by misconfiguration, including the following typical reasons:

- deletion of the NS RRs by the expiration of DNS registry subscription [*5] ;
- NS RRs are not directed to the appropriate servers; and
- A/AAAA RRs do not point the correct IP addresses of the servers listed in the NS RRs.

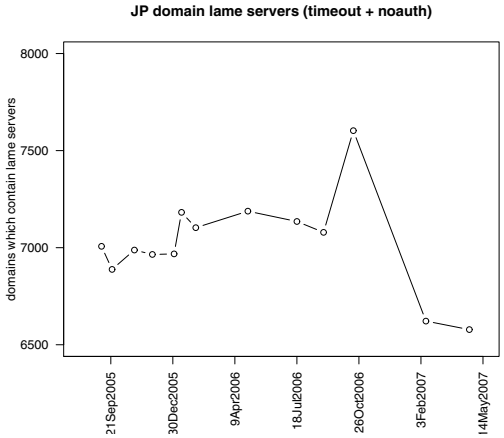

Fig. 1 Numbers of lame-delegated domains under `.jp` ([46], source data used by permission.)

An DNS trace measurement in 2003 [45] shows that the percentage of lame-delegated zones in `.com`, `.edu`, `.net` and `.org` generic Top-Level Domains (gTLDs) were about $15 \sim 20\%$, while `.kr`, `.tw` and `.cn` were even higher.

Suzuki [46] performed the active analysis of lame delegation within `.jp` zone, by comparing the results of non-recursive answers from `.jp` authoritative servers and the second-level `.jp` domain servers. The analyses data shown in Fig. 1 were those performed from September 6, 2005 to April 22, 2007, for 13 times. The total numbers of domains analyzed were decreased from 51819 to 49695 during the period, respectively. The percentage of lame-delegated domains were between $13 \sim 15\%$. This result suggests that the lame delegation rate is stable and not likely to decrease. Suzuki [46] also reports that 87 second-level `.jp` domains still have non-existent domains in the NS RRs which may cause domain hijacking without being detected by the domain owner, as of April 22, 2007.

Pappas et al. [47] shows two other popular types of DNS misconfiguration as follows:

- *diminished server redundancy* : multiple authoritative servers being placed in the same network prefix, so that

*3 : Osterweil et al. [43] proposes an introduction of explicit signing key revocation method by announcing revoked keys as RRs.

*4 : A lame delegation is a situation which the DNS server pointed by NS RRs for a zone do not serve the authoritative data for the zone.

*5 : On May 2005, `e-ontap.com`, which had the authoritative servers running for `visa.co.jp` and other related domains, was found non-existent. Suzuki [44] took over the control of `e-ontap.com` to prevent further possible domain abuse and hijacking.

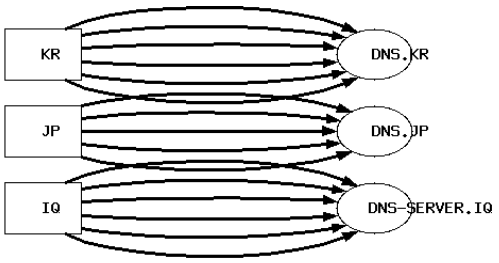

Fig. 2 TLD delegation map [48]: simple delegation to authoritative servers within the zone.

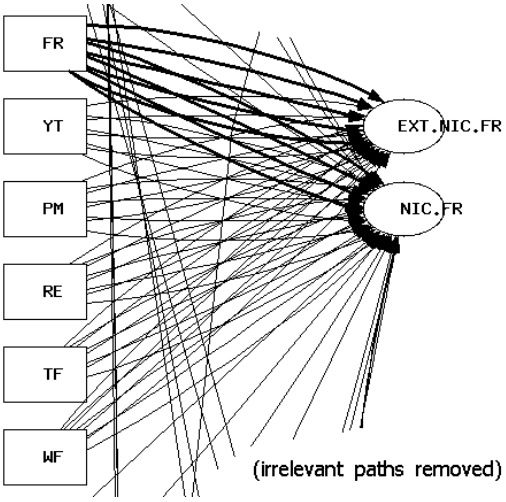

Fig. 3 TLD delegation map [48]: ccTLD for French territories which are dependent to `.fr` servers.

the redundancy supposed to be provided by routing diversity is lost; and

- *cyclic zone dependency* : a situation which name resolution within zone Z_1 requires the resolution of a name in zone Z_2, and the name resolution within zone Z_2 requires the resolution of a name in zone Z_1.

We should also state that introduction of DNSSEC will reveal the inconsistencies of DNS delegation, since DNSSEC-enabled DNS servers actively verify the delegation trees and treat them as errors.

3. 2. Increasing level of indirection

Some domains are increasing level of indirection by cascading multiple delegations. Analyzing Root Zone data as a directional graph describes how complex the inter-domain delegations are formed.

For example, some country-code Top-Level Domains (ccTLDs) have rather simpler structures to keep the authoritative NS RR labels within the zone (Fig. 2). Figure 3 shows some ccTLDs such as those of French external territories [*6] are controlled under the servers of `nic.fr`. Another example

*6 : The ccTLDs `.yt` (Mayotte), `.pm` (Saint Pierre and Miquelon), `.re` (Réunion), `.tf` (French Southern Territories), and `.wf` (Wallis and Futuna) are all of French territories [49].

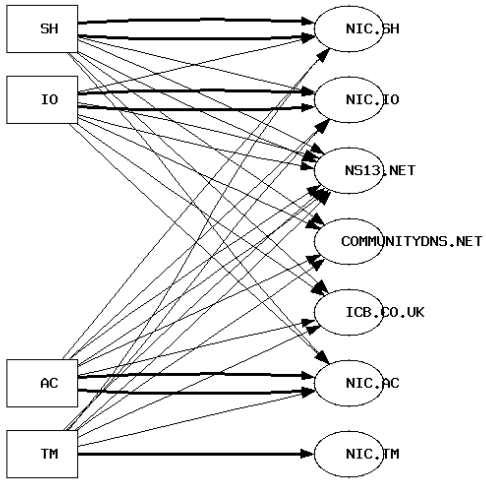

Fig. 4 TLD delegation map [48]: co-delegation which suggests the alliance between multiple ccTLDs.

in Fig. 4 suggests an alliance of operation between different ccTLDs, shown by the co-delegation of zones with each other.

3. 3. Misdirected traffic to The Root Servers

Lots of unresolvable requests are directed to Root Servers, such as:

- PTR RR queries for the RFC1918 [50] private IPv4 addresses, which have no globally-defined answer, whose traffic is now off-loaded by AS112 Project [51];
- incomprehensive strings as domain names, such as search keywords, directly sent from Web browsers; and
- queries to private Top-Level Domains (TLDs), such as `.local`, whose queries was 23.3% of unresolvable TLDs sent to the Root servers in November 2002 [52].

Kato and Sekiya [52] reports only 0.2% of the queries sent to the Root Servers are legitimate (i.e., 99.8% of the queries contain invalid TLDs). Most of the misdirected traffic is preventable by appropriate configuration of end users and ISPs.

3. 4. DNS amplification attack

DNS amplification attack [53] is an attack with spoofed source IP address and using DNS servers and caches as the reflectors [54]. This enables attackers to send a small-size query and send back a large-size answer to the spoofed address, so it *amplifies* the size of attacking packets. The following list of misconfiguration are typical causes of the attacks:

- lack of IP-level ingress/egress filtering [55], [56], on end users and ISPs; and
- *open resolvers* [57], which accept queries from anywhere in the Internet, allowing attackers to inject address-spoofed queries and malicious contents.

3. 5. DNS spoofing

DNS spoofing is an attack to inject a false set of DNS RRs to

DNS cache servers, so that the cache users receive the malicious set of information, presumably leading to misdirection to the attacker's Web site. The following configuration restrictions contribute to this attack:

- DNS query has its own transaction identifier for each query, but the identifier has only 16 bits and cryptographically predictable in some versions of BIND [58] software [59]. The predictability enables injection of malicious data to the DNS caches.
- Many DNS resolvers use predictable source port numbers for each query, whose behavior defined by the operating system implementation. Randomizing the source ports will mitigate the risks, which has already been done by djbdns [60], but still not a well-known practice.
- Short TTLs (<600 seconds) make the caches prone to injection by external attackers. It may also cause unnecessary traffic increase and making the servers weak to denial-of-service (DoS) attacks [61].

4. Conclusions: what to do for the future

We described the examples of existing security issues of DNS, focused on the operational perspectives. We need to emphasize that many of the problems in this paper have been well-known for a long time, and that solving them are heavily dependent on well-trained human DNS operators. While DNSSEC will help preventing DNS spoofing and formalize the zone delegation checking procedures, it will not be the ultimate solution for the persistently existing issues, such as delegation inconsitencies and open resolvers. We propose the following actions to take for securing the DNS and ensuring the reliable operation.

4.1. Our proposals

End users and ISPs should employ the preventive actions against overloading the Root Servers and becoming the DoS attackers by themselves. For example, enforcing ingress/egress IP-address filtering policy, incorporating local resolution mechanisms for non-global IP addresses and domain names, and prohibiting open resolvers, will significantly reduce the unnecessary traffic to the Root Servers and harden the platform against possible DoS-launching attempts.

Automatic crawlers of DNS zone delegation should be introduced by regional DNS registries and supervising organizations (e.g., JPRS, APNIC), to notify lame and inconsistent delegations, and to take penalty actions if the detected inconsistencies are not resolved in a timely manner. The crawlers can also be used to obtain the credibility of the zone, by including but not limited to, the status of co-delegation with other zones, levels of indirection, availablity and vulnerability metrics of the authoritative servers.

Legal and educational supports for maintaining DNS and Internet stability are essential for the sustainable operation. ISPs are as responsible as the end users; ISPs should empower the end users to correctly configure their systems, and monitor them for proper operation. If an attacker emerges from an ISP network, the ISP should immediately react to block the attacker's traffic. This sort of cooperation rarely exists in current ISP-user relationship. We warn that Internet will collapse and become defunct in a near future if end-user and ISP coordination for the sustainable operation keeps failing.

Acknowledgements

Our thanks go to Youki Kadobayashi, Yoshiaki Hori, Eisaku Yamaguchi, Akio Hasegawa, and Hiroki Takakura for their valuable suggestions and comments.

References

[1] P.V. Mockapetris, "Domain names – concepts and facilities," 1987. RFC1034 (also STD13).
[2] P.V. Mockapetris, "Domain names – implementation and specification," 1987. RFC1035 (also STD13).
[3] R. Elz and R. Bush, "Clarification to the DNS specification," 1997. RFC2181.
[4] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," May 2007. RFC4871.
[5] M. Wong and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1," April 2006. RFC4408.
[6] T. Ylonen and C. Lonvick (Editor), "The Secure Shell (SSH) Protocol Architecture," Jan. 2006. RFC4251.
[7] J. Schlyter and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints," Jan. 2006. RFC4255.
[8] S. Kent and R. Atkinson, "Security architecture for the internet protocol," 1998. RFC2401.
[9] M. Richardson, "A Method for Storing IPsec Keying Material in DNS," March 2005. RFC4025.
[10] S. Josefsson, "Storing Certificates in the Domain Name System (DNS)," March 2006. RFC4398.
[11] A. Gulbrandsen and P. Vixie and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)," Feb. 2000. RFC2782.
[12] P. Faltstrom, "E.164 number and DNS," Sept. 2000. RFC2916.
[13] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS," Oct. 2002. RFC3401.
[14] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm," Oct. 2002. RFC3402.
[15] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," Oct. 2002. RFC3403.
[16] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application," Oct. 2002. RFC3404.
[17] R. Droms, "Dynamic Host Configuration Protocol," 1997. RFC2131.
[18] R. Droms (Editor), J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," 2003. RFC3315.
[19] M. Stapp and B. Volz and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option," Oct. 2006. RFC4702.

[20] M. Stapp and B. Volz, "Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients," Oct. 2006. RFC4703.
[21] B. Volz, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option," Oct. 2006. RFC4704.
[22] M. Stapp and T. Lemon and A. Gustafsson, "A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)," Oct. 2006. RFC4701.
[23] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system (DNS UPDATE)," 1997. RFC2136.
[24] J. Klensin, "Role of the Domain Name System (DNS)," February 2003. RFC3467.
[25] D. Atkins and R. Austein, "Threat Analysis of the Domain Name System (DNS)," August 2004. RFC3833.
[26] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," March 2005. RFC4033.
[27] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions," March 2005. RFC4034.
[28] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Protocol Modifications for the DNS Security Extensions," March 2005. RFC4035.
[29] P. Vixie, "Extension Mechanisms for DNS (EDNS0)," 1999. RFC2671.
[30] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, "DNS extensions to support IP version 6," 2003. RFC3596.
[31] Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC), "Testing Firewalls for IPv6 and EDNS0 Support," Jan. 2007. SSAC Report SAC 016, http://www.icann.org/committees/security/sac016.htm.
[32] K. Rikitake, A Study of DNS Transport Protocol for Improving The Reliability, Ph.D. dissertation, Graduate School of Information Science and Technology, Osaka University, Osaka, Japan, Dec. 2004. Public Release Version 1.0, http://www.ne.jp/asahi/bdx/info/depot/dnstransport-phd-v10-pub.pdf.
[33] E. Nordmark and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," October 2005. RFC4213.
[34] R. Draves, "Default Address Selection for Internet Protocol version 6 (IPv6)," February 2003. RFC3484.
[35] Y. Morishita and T. Jinmei, "Common Misbehavior Against DNS Queries for IPv6 Addresses," May 2005. RFC4074.
[36] WIDE Project MAWI Working Group, "Dual-Stack Path Analysis." http://mawi.wide.ad.jp/mawi/dualstack/.
[37] K. Cho, M. Luckie, and B. Huffaker, "Identifying IPv6 network problems in the dual-stack world," NetT '04: Proceedings of the ACM SIGCOMM workshop on Network troubleshooting, New York, NY, USA, pp.283–288, ACM Press, 2004.
[38] IETF dnsext WG, "DNS Extention (dnsext) Working Group Charters." http://www.ietf.org/html.charters/dnsext-charter.html.
[39] DNSSEC Deployment Initiative, "DNSSEC This Month." http://www.dnssec-deployment.org/news/dnssecthismonth/current/.
[40] Internet Assigned Numbers Authority (IANA), "DNSSEC STATUS (experimental)." https://ns.iana.org/dnssec/status.html.
[41] RIPE NCC, "RE: RIPE Community Request for ICANN to Sign DNS Root." http://www.ripe.net/ripe/wg/dns/icann-root-signing.pdf.
[42] B. Laurie, G. Sisson, R. Arends, and D. Blacka, "DNSSEC Hashed Authenticated Denial of Existence." INTERNET-DRAFT draft-ietf-dnsext-nsec3-11.txt.
[43] E. Osterweil, V. Pappas, D. Massey, and L. Zhang, "Zone State Recovation for DNSSEC," Proceedings of the ACM SIGCOMM 2007 Workshops, pp.153–160, Aug. 2007. LSAD'07 Workshop, ISBN 978-1-59593-785-8/07/0008.
[44] T. Suzuki, "VISA domains problem." http://www.e-ontap.com/detail.html.
[45] V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, and L. Zhang, "Impact of configuration errors on DNS robustness," SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, New York, NY, USA, pp.319–330, ACM Press, 2004.
[46] T. Suzuki, "The Critical Situation of DNS," Proceedings of FIT2007 (6th Forum on Information Technology) Bumber 4, pp.29–31, 2007.
[47] V. Pappas, P. Fältström, D. Massey, and L. Zhang, "Distributed DNS troubleshooting," NetT '04: Proceedings of the ACM SIGCOMM workshop on Network troubleshooting, New York, NY, USA, pp.265–270, ACM Press, 2004.
[48] T. Suzuki, "TLD authorities map." http://www.e-ontap.com/dns/map/.
[49] Internet Assigned Numbers Authority (IANA), "Root-Zone Whois Information." http://www.iana.org/root-whois/index.html.
[50] Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, and E. Lear, "Address Allocation for Private Internets," February 1996. RFC1918.
[51] AS112 Project, "AS112 Project)." http://public.as112.net/.
[52] A. Kato and Y. Sekiya, "Analysis of DNS Traffic at a DNS Server in an ISP," IEICE Trans. Commun. (Japanese Edition), vol.J87-B, no.3, pp.327–335, March 2004.
[53] R. Vaughn and G. Evron, "DNS Amplification Attacks (*Preliminary Release*)." Dated March 17, 2006, http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.
[54] V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks," Computer Communication Review, vol.31, no.3, pp.38–47, 2001.
[55] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," May 2000. RFC2827.
[56] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," March 2004. RFC3704.
[57] J. Damas and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks," July 2007. INTERNET-DRAFT draft-ietf-dnsop-reflectors-are-evil-04.txt.
[58] Internet Software Consortium, "BIND." http://www.isc.org/bind/.
[59] A. Klein, "BIND 9 DNS Cache Poisoning." http://www.trusteer.com/docs/BIND_9_DNS_Cache_Poisoning.pdf.
[60] D. J. Bernstein, "djbdns." http://cr.yp.to/djbdns.html.
[61] V. Pappas, D. Massey, and L. Zhang, "Enhancing DNS Resilience against Denial of Service Attacks," Proceedings of The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DNS2007), 2007. http://www.cs.ucla.edu/~lixia/papers/07DSN_TTL.pdf.