Critical Infrastructure Protection Standard for Canadian Telecommunications Service Providers (CTSPs)

V1.1 January 20, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group

for

Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)

Contents

Revision History

The following table highlights edit changes to the document.

Editor	Date	Notes
CTCP Architecture Committee	May 30, 2019	Content creation
Kevin Miller, SaskTel	June 1, 2019	Draft started
Kevin Miller, SaskTel	July 30, 2019	Continued work on draft
Marc Kneppers, TELUS	January 20, 2020	Minor updated based on stakeholder feedback
Marc Kneppers, TELUs	March 31, 2020	Final edit for consistency, accuracy, and readability

The following table highlights major content or policy changes to the document.

Section	Contribution	Date
SS7	A general recommendation to adhere to GSMA SS7 best practices for monitoring and mitigation SS7 attacks was included as a new best practice.	March 13, 2019
BGP	A summary of Internet best practices and what is currently common and appropriate for Canadian operators.	March 13, 2019
DNS	Best practices for DNS implementation and operations, in more detail than previous.	March 13, 2019
Response	Recognition of our role in being good netizens was added. Section 5.2.1 and 5.3 add the responsibility of CTSPs for attacks that initiate in their network space and creates the expectation that CTSPs will monitor and mitigate outbound attacks that will affect other Internet entities.	March 13, 2019
Awareness	Employee and Customer cyber security awareness was added as a best practice.	April 10, 2019
Privacy	Privacy expectations with reference to applicable federal statutes were added.	February 13, 2019
Virtualization	Virtualization best practices added to section 3.1.5.	April 10, 2019

1. Critical Infrastructure Protection Standards

1.1 Network Architecture and Design

The Network Architecture and Design section of this standard define recommended controls for Critical Infrastructure[1] Providers. Critical Infrastructure providers implementing these controls are helping to protect Canadians.

1.1.1 Network Segmentation Controls:

CTSPs should have the capability to:

1. Ensure that the management, control and user planes are;
    a. At a minimum, logically separated, and
    b. Preferably, physically separated as well.
2. Provide diagrams demonstrating plane separation within their network infrastructures.

1.1.2 Management Plane Controls:

CTSPs should have the capability to:

1. Isolate device and operational management functions and restrict access to these from only the management plane.
2. Restrict access, allowing access to only known and approved hosts and services (whitelisting).
3. Use secure management protocols whenever possible.
4. Log critical events for network elements.
5. Investigate malicious events/security incidents.

1.1.3 Control Plane Controls:

CTSPs should have the capability, for all forms of control plane signalling, to:

1. Validate all signalling partners (e.g. BGP peering/transit, SIP trunk, etc).
2. Validate all input from signalling partners.
3. Drop all signalling from sources that are not signalling partners.
4. Prevent signalling points from being addressable outside of the Control Plane layer.

[1] Public Safety Canada, “Critical Infrastructure”, June, 2019, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx; retrieved March 31, 2020

5. Implement mechanisms to prevent signalling sessions from being disrupted (e.g. authentication mechanisms, network segmentation, etc).
6. Implement mechanisms to protect wireless control channels and signalling traffic towards users.
7. Implement mechanisms to validate the end devices on their networks to ensure that no unauthorized devices are able to connect.
8. Implement egress filtering controls.
9. Monitor and prevent signalling abuse

1.1.3.1 BGP-specific Interconnection Controls:

CTSPs should have the capability, in addition to the broad control plane signalling protections (1.1.3), to:

1. Manage route resources and ensure the integrity of their own advertised information.
2. Protect the BGP speaker with interface packet filters and/or control-plane filters (to protect CPU resources on the router).
3. Protect TCP session using SHAM-SHA/HMAC-MD5, configured at both ends of the session with shared secret.
4. Implement the TTL hack (RFC5082) at peering or in IXP scenarios.
5. Prevent spoofed BGP packets by blocking packets sourced from the CTSP's own IP space at edge of network.
6. Employ general BGP prefix filtering (generally inbound, but can be applied outbound for safety):
    a. filter out special-purpose prefixes, not globally routed
    b. filter out unallocated prefixes (mostly IPv6 in current address space utilization)
    c. filter out overly specifics (generally, /24 and /48 for IPv6)
    d. filter out the default route
7. Employ peer/upstream prefix filtering:
    a. filter out local AS prefixes
    b. filter out IXP LAN prefixes
8. Employ customer prefix filtering (per customer):
    a. only accept known customer prefixes
    b. filter out the default route
    c. filter out overly specific routes
    d. filter out prefixes not globally routed
9. Input all CTSP route entries into the IRR (Internet Route Registry) to protect against automatic filter creation.
    a. Create an organizational entry/presence
    b. Ensure data is up to date

   c. Ensure that your prefixes are present and not claimed by another organization.
10. Ensure maximum prefix limits are defined for each peering session.
11. Employ AS Path filtering:
    a. Accept customer routes with only allowed ASNs in the path
    b. Do not accept routes with private ASNs
    c. Do not accept routes without customer ASN as path origin (unless a known downstream ASN has been identified)
    d. Do not accept routes with transit or upstream ASNs in AS Path
    e. Reject BGP routes from our customers with Tier1 transit AS numbers in the AS Path[2]
    f. Drop customer BGP routes with bogon AS numbers in the AS Path
12. Ensure BGP communities received from peers and customers are filtered:
13. scrub inbound communities with their number in the high-order bits ("community set")
14. Scrub outbound communities to remove internal policy indicators
15. Don't scrub standard communities meant for transmission (e.g. "no export"), notably the Black Hole community if in use across peering[3].
16. Implement the following peering security controls
    a. Peering should be done on each interface in an isolated subnet which is not advertised in the general routing table (CSRIC)
        i. There is an obvious exception for public Internet Exchange connections where a shared subnet is used between multiple peers solely for the purpose of peering
    b. For multi-hop sessions, only relevant BGP Peering IPs should be advertised to peering partners
    c. Neighbour BGP session status changes should be logged
    d. Use a separate MD5 password per session, or per administrative domain
    e. The use of different MD5 passwords may have different costs, depending on your operational model, which may remove some of its value[4].
        i. This is discussed in depth in CSRIC report[5].

[2] Snijders, Job, "Practical everyday BGP filtering with AS_PATH filters: Peer Locking", https://www.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf; retrieved April 24, 2018
[3] King, T, Dietzel, C, Snijders, J, Doring, G, Hankins, G, "BLACKHOLE BGP Community for Blackholing Draft-ymbk-grow-blackholing-01", July 29, 2015, https://tools.ietf.org/id/draft-ymbk-grow-blackholing-01.html; retrieved May 20, 2018
[4] Gilmore, P, et al, "MD5 considered harmful", https://mailman.nanog.org/pipermail/nanog/2012-January/thread.html#44499, January 2012; retrieved April 25, 2018
[5] CSRIC (The Communications Security, Reliability and Interoperability Council), "FINAL Report – BGP Security Best Practices", http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf, March 2013; retrieved April 9, 2018

f. Use of link-local addresses in IPv6 to isolate peering addresses from general reachability (CSRIC).
g. Use of Black Hole BGP Community[6] or flowspec for inter-provider signalling during security (sample tool: ExaBGP[7])

17. Discarded BGP packets due to invalid secret or parameters should be logged/counted.
18. Utilize BGP communities should be used to customize the use and propagation of network subnets. Examples include limiting subnet advertisement to regions, or for limited purposes, and identifying traffic behavior (null route, etc)
19. Adopt the standard community value of 65535:666 for BGP Black Holed routes
20. Configure next-hop manipulation for threat mitigation:
    a. Utilize remotely triggered Black Hole functions – ensure that all BGP speakers have a 'null route' IP address that can be used as next-hop in prefix advertisements, causing traffic to be dropped on every router when tagged with the Black Hole community.
    b. Utilize BGP sinkhole functions – ensure that all BGP speakers have a reachable IP address that can be used as next-hop in prefix advertisements, causing traffic to be re-routed to a centralized analysis system. Use of this sinkhole is controlled by prefix advertisement tagged with a unique community value.
21. Require a LOA[8] from customers proving their ownership of the IP space they wish you to advertise for them.
22. Monitor the BGP service for hijacking of their own ASN space
23. Monitor the public Internet Route Registry for hijacking or manipulation of their route registry objects
    a. Query IRR for your own prefixes, flag anything that doesn't come from your organization's "maintainer-ID"

1.1.3.2 SS7 (Signalling System 7), Diameter and 5G inter-provider signalling Controls:

SS7 has traditionally been the primary signalling protocol between voice providers. Both Diameter and 5G inter-provider signalling provide similar functions to SS7 signalling and must be appropriately protected. Diameter is specific protocol used across many mobility networks and evolutions. In 5G, a new signalling scheme is introduced between providers which uses HTTPS as the transport. An evaluation of these methods is

[6] King, T, Dietzel, C, Snijders, J, Doring, G, Hankins, G, "BLACKHOLE BGP Community for Blackholing Draft-ymbk-grow-blackholing-01", July 29, 2015, https://tools.ietf.org/id/draft-ymbk-grow-blackholing-01.html; retrieved May 20, 2018
[7] ExaBGP Wiki, https://github.com/Exa-Networks/exabgp/wiki; retrieved May 25, 2018
[8] https://blog.apnic.net/2014/10/15/the-good-practice-of-legitimacy-of-address-loa-checks/

provided by the FCC CSRIC5-WG10 working group[9].

CTSPs should have the capability, in addition to the broad control plane signalling protections (1.1.3), to:

1. Perform appropriate (stateless) filtering on Signal Transfer Points (STPs) to restrict use of SS7 commands to only legitimate use
2. Where STP filtering is not possible, perform additional (stateless and stateful) filtering via SS7 firewall.
3. Additionally, implement secondary functional filters where possible or appropriate on connected services, such as on the SMS routers, SMSC, or HLR.
4. Follow GSMA SS7 security recommendations[10]:
    a. FS.07[11] – SS7 and SIGTRAN Network Security
    b. FS.11[12] – SS7 Interconnect Security Monitoring and Firewall Guidelines
    c. IR.82[13] – SS7 Security Network Implementation Guidelines
5. Apply Network segmentation industry best practices i.e. SMS Home routing
6. Configure NE to ignore malicious SS7/Diameter/HTTP(5G) messages
7. Subscribe to signalling threat feeds (e.g. GSMA, etc…)
8. Develop operational procedures to react to security incidents

1.1.4 Data Plane Controls:

CTSPs should have the capability to:

1. Validate the integrity of external traffic entering their network wherever possible.
2. Prevent traffic from spoofed (false originator) devices or sources from entering

[9] "CSRIC5-WG10-FinalReport031517.pdf", https://www.fcc.gov/file/12153/download
[10] To request access to these documents please contact the GSMA: https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group
[11] FS.07, https://infocentre2.gsma.com/gp/wg/FSG/OfficialDocuments/Forms/OfficialDocument/docsethomepage.aspx?ID=241&FolderCTID=0x0120D5200072B7664C9B6C41A5A2203ED59788C6B200B7DD38F151D844A683065B0BA90F5F8A0088082DAE9175764D8C5539F31B70A521&List=0f9a1609-e8d8-4a68-8486-502bde84541a&RootFolder=/gp/wg/FSG/OfficialDocuments/FS.07%20SS7%20and%20SIGTRAN%20Network%20Security%20v4.0%20(Current)
[12] FS.11, https://infocentre2.gsma.com/gp/wg/FSG/OfficialDocuments/Forms/OfficialDocument/docsethomepage.aspx?ID=286&FolderCTID=0x0120D5200072B7664C9B6C41A5A2203ED59788C6B200B7DD38F151D844A683065B0BA90F5F8A0088082DAE9175764D8C5539F31B70A521&List=0f9a1609-e8d8-4a68-8486-502bde84541a&RootFolder=/gp/wg/FSG/OfficialDocuments/FS.11%20SS7%20Interconnect%20Security%20Monitoring%20and%20Firewall%20Guidelines%20v4.0%20(Current)
[13] IR.82, https://infocentre2.gsma.com/gp/wg/IR/OfficialDocuments/Forms/OfficialDocument/docsethomepage.aspx?ID=582&FolderCTID=0x0120D5200072B7664C9B6C41A5A2203ED59788C6B200B7DD38F151D844A683065B0BA90F5F8A00EE7A3E0638A40E42B586D4C20B08AFCE&List=50ea34d5-ec5d-4271-b8ca-a2ce4303a79d&RootFolder=/gp/wg/IR/OfficialDocuments/IR.82%20SS7%20Security%20Network%20Implementation%20Guidelines%20v5.0%20(Current)

their network.
3. Prevent malicious or inappropriate traffic from entering their network. These measures include protocol, address or volume filters.
4. Prevent volumetric attacks (i.e. attacks that attempt to exceed network or device bandwidth) from affecting their infrastructure.
5. Ensure that management resources and infrastructure networks cannot be targeted by data plane traffic.
6. Use traffic restrictions based on a “blacklist” approach, where all traffic is allowed by default, but the CTSP has the ability to block (or blacklist) malicious or inappropriate traffic as necessary.
7. Track malicious traffic to the originating source on their network, or to the point of entry to their network.
8. Correlate traffic sourced on their network to individual customers.
9. Ensure the integrity of traffic leaving their networks.
10. Implement mechanisms to prevent traffic with invalid characteristics.
11. Behave as responsible network citizens and take steps to avoid harm to other networks.
12. Respond to reasonable external complaints from their networks about cases of abuse that have not been prevented.

1.1.5 Virtualization Controls:

CTSPs should have the capability to:

1. Physically isolate (i.e. do not virtualize) services susceptible to side channel attacks (e.g. cryptographic services and certificate authorities).
2. Assess the need for co-locating virtualized systems belonging to different organizations.
3. Use bare-metal hypervisors.
4. Physically separate hypervisor networks (e.g. data, management, storage, and live migration) from other networks (e.g. VM management networks) and from each other, and ensure they do not bridge multiple security zones.
5. Do not co-locate Virtual Machines (VMs) with different security requirements on the same hypervisor and ensure they do not bridge multiple security zones.
6. Do not host virtualized security functions on the same infrastructure as the systems they are protecting and physically segregate security functions that bridge multiple security zones.
7. Use logical security controls (e.g. micro segmentation firewalls, VLANs) for effective network access controls within security zones and/or hypervisors.
8. Create dedicated management roles for virtualized systems and per security zone.

9. Implement strict resource allocation policies for VMs.
10. Use introspection or similar technologies to protect VMs.
11. Implement strict image management policies to mitigate VM sprawl, including rogue and dormant VMs.
12. Implement strict physical and logical access control policies and/or encryption to mitigate VM theft.
13. Ensure that hypervisors VMs, and virtualized network functions follow the same rules and non-virtualized systems (e.g. defense-in-depth):
    a. Network segmentation (see 1.1.1 - Network Segmentation)
    b. Plane separation (See 1.1.2 - Management Plane, 1.1.3 - Control Plane, 1.1.4 - Data Plane)
    c. Hardening (See 1.2.1 - System and Component Hardening)
    d. Secure sensitive communications (e.g. encryption and authentication)
    e. Update/patch management (e.g. update early and often)
    f. Managed service provider access controls (See 1.2 – "CSTAC Vendor Management for CTSPs v1.1"[14])
    g. Network access control (e.g. implement strict network access policies)
    h. Regular security testing (See 1.3 Security Testing)
    i. Logging and monitoring (See " CSTAC Network Security Monitoring and Detection Standard for CTSPs v1.0"[15])

[14] CSTAC Best Practices documentation, CSTAC, https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html; retrieved January 20, 2020
[15] CSTAC Best Practices documentation, CSTAC, https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html; retrieved January 20, 2020

1.2 Security Controls for Core Equipment

The Security Controls for Core Equipment section of this standard define recommend controls for Critical Infrastructure Providers. Critical Infrastructure providers implementing these controls are helping to protect Canadians.

1.2.1 General System and Component Hardening Controls:

Basic device hardening should be employed according to vendor guides and industry-recognized best practices, which are not listed in full here but include the following.

CTSPs should have the capability to:

1. Implement system and device hardening guides published by reputable organizations for more detailed recommendations on the hardening of various types of systems and devices[16].
2. Choose an industry-recognized hardening standard or develop in-house standards that meet the same level of effectiveness as recognized public standards and mandate the use of these standards within their organizations.
3. Mandate hardening requirements for third party service providers through contractual obligations relating to the provision and maintenance of services.

1.2.2 Domain Name System (DNS) Hardening and Security Controls:

CTSPs should have the capability to:

1. Identify DNS critical infrastructure and services.
2. Ensure that they are deploying, configuring, and securing DNS infrastructure and services according to industry-recognized standards.
3. Protect their domain as well as all other domains for which they are responsible.
4. Identify valid contact information in authoritative sources.
5. Protect name service integrity for customer data plane, management plane and control plane in consideration of the presence of adversaries on each.
6. Detect and contain disruption that could affect customers or other service providers.
7. Respond to abuse queries in a timely and collaborative fashion.
8. Recover from attacks and abuse of authoritative and resolving DNS through resilience such geographically diversity and other techniques.

[16] NIST, “Secure Domain Name System (DNS) Deployment Guide”, SP-800-81-2, Section 8, September, 2013, https://csrc.nist.gov/publications/detail/sp/800-81/2/final; retrieved March 31, 2020

1.2.3 DNS Service Protection Controls

1.2.3.1 Internal Namespace

CTSPs should have the capability, within their own internal organizations, to:

1. Identify namespace necessary to operate as a standard employee or contractor of the business, as a telecommunications systems service provider, as a subscriber, and as a public person interacting with the service provider.
2. Enable activities in their correct context by describing network security zones, define namespace resolution “horizons” visible from each zone, and the namespace each horizon should be able to resolve.
3. Align namespace resolution to the current zone, plus lower sensitivity zones if required. For example, a provisioning system may require accessing a system for patching but not for general web browsing, so the horizon should be limited through filtering.
4. Define the namespace that should be accessible from different security zones to clearly identify normal name lookup patterns for designers within the organization. Use a table such as one shown below. CTSP provisioning infrastructure should be very carefully considered (emphasis):

Namespace Zone/User	CTSP Service Names	Customer Service Names	Internet Service Names
Internet	No	No	Yes
DMZ servers	No	Limited	Yes
Customer users	No	Yes	Yes
Customer operations	Limited	Yes	Yes
CTSP operations	Yes	Limited	Limited

Namespace Zone/User	CTSP Provisioning Plane	CTSP Control Plane	User Plane
Internet	No	No	Yes
DMZ servers	No	Limited	Yes

Customer users	No	No	Yes
Customer operations	Limited	No	Yes
CTSP operations	Yes	Yes	Limited

1.2.3.2 Management

CTSPs should have the capability to:

1. Implement awareness programmes within their organizations for DNS security features and functions, using this document as a basis.
2. Inventory DNS realms and assess them for security maturity.
3. Communicate to first response and incident handler teams the existence of new DNS realms.
4. Provide security assessment, review, and improvement services for DNS realms.
5. Assemble libraries for the reuse of techniques used in improved deployments.

1.2.3.3 5G Mobility

CTSPs should have the capability to:

1. Implement DNS architecture in the evolved packet core that aligns with the architecture proposed in this document or a similar architecture
2. Disallow resolution traffic to arbitrary DNS servers outside the evolved packet core
3. Restrict DNS traffic via firewall rules to known, trustworthy forwarders in the evolved packet core

1.2.3.4 User Equipment Plane Resolution

CTSPs should have the capability to:

1. Implement DNS architecture in the evolved packet core that aligns with the architecture proposed in this document or similar architecture
2. Disallow resolution traffic to arbitrary DNS servers outside the evolved packet core
3. Restrict DNS traffic via firewall rules to known, trustworthy forwarders in the evolved packet core
4. Employ DNS filtering or payload inspection to reduce the chances of poisoned answers
5. Employ DNSSec as described in the DNS Cryptography section

1.2.3.5 Mobility Plane Separation

Signalling information should not be exposed to the UE resolution plane.

An example is the E164 Number to URL Mapping (ENUM) mechanism which uses DNS services but is not intended for widespread exposure. This scheme stores telephone number data in the e164.arpa DNS zone so that voice calls can be placed between legacy and more modern call networks.

CTSPs should have the capability to:

1. Differentiate the use of public or user ENUM data from private or carrier ENUM to avoid unwanted robot enabled calling.
2. Avoid mixing private and public authority namespace data.
3. Avoid mixing signalling and user namespace data and services.
4. Avoid control plane servers being accessible to the UE.
5. Avoid exposure of the control/equipment DNS zones to other resolution planes or horizons.
6. Avoid exposure of the e164.arpa DNS zone to other resolution planes or horizons.
7. Populate the control/equipment and e164.arpa DNS zone via similar out-of-band mechanisms described for enterprise configurations where the DNS zone servers receive their data as built on the management plane.

1.2.3.6 DNS Resiliency across Services

Multiple techniques can be used to ensure resiliency of the DNS service. First, the service is deployed on a minimum of two servers so that a single failure does not cause an interruption of the service. In addition, the service is normally deployed at a minimum of two geo-diversified sites, so the service is resilient in case of a major disaster such as a fire or earthquake.

In order to support the geo-diversity without affecting the efficiency of the service, the IP Anycast[17] addressing scheme is used. IP Anycast is a network addressing and routing method where a single address has multiple routing paths to multiple endpoint destinations. Routers select the best path based on different network parameters including latency measurements.

Normally, a minimum of 2 IP Anycast addresses are supplied to the client. They could be IPv4, IPv6 or a combination of the two.

[17] Abley, J, and Lindqvist, K, “Operation of Anycast Services”, BCP 126, IETF Network Working Group, December, 2006, https://tools.ietf.org/html/rfc4786; retrieved March 31, 2020

CTSPs should have the capability to:

1. Deploy DNS in a resilient configuration, consisting of a minimum of two servers
2. Deploy the DNS service at a minimum of two geo-diversified sites
3. Deploy the DNS service using IP Anycast
4. Configuring DNS authority servers on addresses within Anycast network prefixes to take advantage of multiple BGP routing paths.

    a. If any AS is multi-homed via different BGP peering points, advertise via diverse peering points such that each advertisement contains different authority servers that host the same authority information. Ensure that the higher-order prefix is advertised at the best peering point for best resilience.
5. Patch the DNS service regularly in order

1.2.3.7 DNS Monitoring

CTSPs should have the capability to:

1. Detect and alert on cybersecurity threats to DNS.
2. Maintain regular DNS monitoring for situational awareness. Specific monitoring should include;
    a. Recursive resolver server monitoring
    b. Authoritative server monitoring
    c. Anycast network traffic monitoring such as Netflow on ingress links
    d. Detect large packets, features such as edns0 traffic direction, IP and DNS payload fragmentation which have low practical utility but high potential for misuse.

1.2.3.8 DNS Configuration Management

CTSPs should have the capability to:

1. Use configuration management for database files that includes version, rollback, locking/merging delta, authorship, and authentication.
2. Treat inclusion of public addresses as exceptions in private namespace.
3. Designate servers that host namespace visible to the public as delegated authority servers.
4. Delegation via NS records point to only these hosts.

1.2.3.9 CTSP Network Considerations for External DNS

CTSPs should have the capability to:

1. Restrict open resolvers on their networks. Inbound traffic to public DNS resolvers, should be limited to the CTSP customers using filters.
2. Separate public authoritative servers into two different network zones: the hidden master authority server behind a firewall and the slaves in a DMZ. Only the authority slaves should be visible from the outside world (Internet)
3. Filter server traffic to/from and between CTSP DNS servers to known entities (protect the signalling plane)
4. Provision DNS with sufficient network capacity to handle traffic bursts
5. Rate limit inbound traffic to the DNS servers
6. Implement anti-spoofing controls on CTSP end-points (generally, but specifically) for the prevention of abuse of CTSP DNS servers

1.2.3.10 DNS Network Considerations for IPv6

CTSPs should have the capability to:

1. Apply all security measures normally used with IPv4 to IPv6 servers
2. Support reverse address translation of IPv6 addresses in the authoritative DNS service.
    a. Static reverse records cannot be provided due to size, so dynamic creation of answers will be required in most cases. CTSP should consider the behaviour of the software when responding to unknown request volumes, and the potential for denial of service or other attacks by adversaries making queries against the infrastructure.

1.2.3.11 DNS Query Logging

CTSPs should have the capability to:

1. Configure DNS servers to perform off-board event logging when necessary using connectionless mechanisms.
    - This allows for performance, storage cost and privacy enhancements by centrally applying filtering and retention policies.
2. Use a passive logging mechanism such as a network tap if performance impact is negative.

1.2.3.12 DNS Cache Poisoning[18]

CTSPs should have the capability to:

[18] Son, Sooel, and Shmatikov, Vitaly, “The Hitchhiker’s Guide to DNS Cache Poisoning “, The university of Texas at Austin; https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf; retrieved March 31, 2020

1. Provide DNS event logs to detect cache poisoning events and origin. Analytic techniques can use these logs to establish normal baseline patterns and identify statistically anomalous systems.
2. Ensure that appropriate data, including DNS query id, source port, source address, and synchronised date/time stamps is provided for collation with other sources.
3. Enable the receiving system to perform proper time analysis with time binding or configuration of the logging for the generating device so that samples can be time analysed.

3.13 DNS Resolver Resiliency

CTSPs should have the capability to:

1. Reduce the potential impact on local networks and neighbouring authoritative servers from denial of service by enabling DNS resolvers to serve expired data during the exceptional circumstance that a recursive resolver is unable to refresh the information[19] (some implementations may call this feature "cache stretching").
    a. The effect is to remember the last known good record and to use this, if the query can not be refreshed (due to DoS), and the TTL has expired. If an affirmative ICMP unreachable is received the record may be queried from a secondary or expunged from the cache.

1.2.3.14 DNS – Defense and Detection Controls

CTSPs should have the capability, in addition to the above recommendations, to:

Defend by;

1. Performing a threat model exercise where the CTSP's DNS servers are used as a reflector[20] or amplifier for traffic volume attacks. Enumerate the most likely and severe threat and address them.
2. Configuring DNS infrastructure against threats that would use it as an attack beachhead and indirect attack staging point[21].

[19] Lawrence, D, Kumari, W, and Sood, P, "Serving Stale Data to Improve DNS Resiliency", draft-ietf-dnsop-serve-stale-01, IETF DNSOP Working Group, 2018, https://tools.ietf.org/html/draft-ietf-dnsop-serve-stale-01; retrieved March 31, 2020
[20] Damas, J, and Neves, F, "Preventing Use of Recursive nameservers in Reflector Attacks", BCP 140, IETF Network Working Group, 2008, https://www.ietf.org/rfc/rfc5358.txt; retrieved March 31, 2020
[21] US Department of Homeland Secuirty, CISA, "Alert(TA13-088A) – DNS Amplification Attacks", March 29, 2013, https://www.us-cert.gov/ncas/alerts/TA13-088A; retrieved March 31, 2020

3. For environments with security perimeters (e.g. Corporate enterprise networks), configuring DNS infrastructure against threats that would use it as a method to exfiltrate data via egress traffic filtering, protocol proxy and "canary" resources to detect the outflow of information.
4. Implement Response Policy Zones (RPZ)[22] technique that enables filtering based on additional information (such as reputation) to make security policy decisions.

Detect by;

1. Enabling query logging to detect lookups associated malicious sites.
2. Procuring threat intelligence feeds that identify malicious sites.

1.2.3.15 DNS - Privacy Protection controls

CTSPs should have the capability to:

1. Perform threat modelling on the organization's DNS infrastructure and use with respect to privacy[23].
2. Ensure that personally identifying information is not included or is filtered from the event log messages.
3. Ensure that target logging systems retain the event logs for only as long as required for normal operational analysis.
4. Assess the sensitivity of information disclosed within DNS traffic in aggregate, as well as at an individual transaction or query-response level.
5. Embed privacy concerns in the DNS organizational policy, implementation standards, and architecture roadmaps.
6. Consider planning and implementing a privacy-enhanced architecture that provides separate data atoms and employs cryptography for confidentiality in addition to integrity.
7. Consider tools and technology with the ability to minimize qualified name (QNAME) RR lookups from sharing Full Qualified Domain Names (FQDNs) with every step of a recursive lookup.
    a. Example: when resolving www.xyz.domain.org, request only domain.org from .org authoritative servers, xyz.domain.org from domain.org authoritative servers and www.xyz.domain.com from xyz.domain.org authoritative servers.

[22] "DNS Response Policy Zones", https://dnsrpz.info/; retrieved March 31, 2020
[23] Bortzmeyer, S, "DNS Privacy Considerations", RFC 7626, IETF, https://tools.ietf.org/html/rfc7626; retrieved March 31, 2020

8. Consider the deployment of tools and technology with the ability to provide confidential name service lookups across untrustworthy WAN, such as the interaction between stub resolvers and recursive forwarders that use DNS over TLS[24], or DNS over HTTPS (DoH)[25].
    a. Monitor the progression of these technologies in browser clients, stub resolvers and DNS server infrastructures and work to enable this privacy within CTSP networks.

1.2.3.16 DNS Cryptography Security and Service Extensions

CTSPs should have the capability to:

1. Consider signing sensitive DNS global top-level domain zone resource records using Domain Name System Security Extensions (DNSSEC[26]) with Next Secure Record Version 3 (NSEC3) and serve Transaction Signature (TSIG) records with zone files.
2. Consider signing their public Internet DNS zone files using Transaction Signature (TSIG) records to ensure that records integrity is maintained for zone data transfers between primary and secondary servers by;
    a. Enumerating a list of hosts authorised to perform zone transfers
    b. Using general TSIG keys that use adequate length and are unique for each set of hosts.
    c. Securing the transmission of the key file between name servers.
    d. Modifying permissions so that only the nameserver account may manipulate the key file.
3. Enable resolvers under their control to validate responses using DNSSEC by;
    a. Surveying all resolvers in path for customers and within the CTSP as an enterprise.
    b. Enable to validate DNSSEC such that the DNS infrastructure will support those end users and resolvers that wish to receive valid answers.
4. Consider signing sensitive DNS global top-level resource records using DNSSEC by;
    a. Identifying the key global second level domains that require authenticity (i.e. domain.ca)

[24] Hu, Z, Zhu, L, Heidemann, J, Mankin, A, Wessels, D, Hoffman, P, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, IETF, https://tools.ietf.org/html/rfc7858; retrieved March 31, 2020
[25] Hoffman, P, McManus, P, "DNS Queries over HTTPS (DoH)", RFC8484, IETF, https://tools.ietf.org/html/rfc8484; retrieved March 31, 2020
[26] ICAAN, "DNSSEC – What Is It and Why Is It Important?", https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en; retrieved March 31, 2020

   b. Identifying the key third level domains that require authenticity (i.e. secure.domain.ca)
   c. Maintaining the Zone signing key and key Signing Key in a protected storage area.
5. Enable DNSSEC so customers can sign their sensitive DNS global top-level domain zones for which they own and control the resource records.
   a. This would also support customers use of DNS-based Authentication of Named Entities (DANE[27]). DANE achieves binding between the DNS and entities that seek to use private/public key cryptography for identification.
6. Consider Certificate Authority Authorization (CAA).
   a. CAA achieves binding between the DNS and public certificate authorities. An HTTPS trust domain may publish those public certificate authorities authorised to issue certificates for an organization's domains.
7. Consider using Sender Policy Framework (SPF) for DNS-enabled email security.
   a. SPF ensures that receiving parties can check to see if a message originated from a legitimate source, using DNS as the verification mechanism.

1.2.3.17 DNS Freedom

CTSPs should have the capability to:

1. Allow subscribers to choose the DNS service that best fits security, privacy and technology needs on their endpoint devices or network gateways.
2. Ensure third party DNS services, that provide additional privacy and security, are properly routed

1.3 Security Testing

1.3.1 Vulnerability Assessment Controls

CTSPs should have the capability to:

1. Include security testing in all system development test plans.
2. Test devices against the hardening security standards adopted.
3. Perform security testing prior to systems being granted approval to move into production.
4. Ensure that network planes are secure by conducting regular risk assessments on each plane to identify and respond to unacceptable risks.

[27] Hoffman, P, and Schlyter, J, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, IETF, https://tools.ietf.org/html/rfc6698; retrieved March 31, 2020

1.3.2 Compliance Monitoring and Audit Controls

CTSPs should have the capability to:

1. Establish a Vulnerability Management Program (VMP) containing processes and tools to scan production systems and network equipment for vulnerabilities.
2. Document processes and procedures for addressing discovered vulnerabilities.
3. Detect when new equipment has been added to networks.

1.4 Change Procedure Controls

CTSPs should have the capability to:

1. Maintain a Change Management Program to ensure that changes to production environments and systems are introduced in a controlled manner to help to mitigate risk and ensure that all changes comply with security requirements.
2. Ensure that the Change Management Program includes a Change Advisory Board (CAB) that has representatives from all impacted areas to ensure that changes are properly reviewed.
3. Ensure that changes are approved by management with direct responsibility for the operations of the components being changed.
4. Ensure that the change control procedures define the testing that is required to validate changes.
5. Ensure that post-change testing is conducted to validate the integrity of all pre-change security controls.

Appendix A – DNS Architectural Design Considerations and Principles

Regardless of how an organization divides its security zones, the basic DNS components assume there are three fundamental network security zones:

A ***corporate network*** is often contained in an ***intranet zone*** which contains an enterprise's resolver client and servers, perhaps split into a client and server sub-zone.

For a CTSP, the corporate network is normally split in two sections:

i. Access Network where the customers access the CTSP network
ii. Core Network where the customer services reside

A ***Public Internet*** zone which contains the public Internet root DNS servers, top level domain (TLD) servers, zone authority (e.g. canada.ca) and any "cloud" services. These are potentially split into different sub-zones belonging to the operators of the various servers and services, interconnected via the global IP internet.

An ***extranet*** or **demilitarized zone** often houses services destined to provide services to the **Public Internet** for the enterprise, or through which to inspect traffic and services consumed on the corporate **intranet**. This zone may also be split up into sub-zones or have extranet services provided on gateways to this zone.

The many different generic DNS components can be overlaid on this basic reference architecture for context. Local customizations will often differ, to suit specific requirements of the enterprise.

Views

A logical security zone view is detailed in Figure 1 and a similar architecture but with a network topological view is shown in Figure 2.

Individual organizations will likely have a standard network security zoning that resembles zoning outlined here. Organizations should follow their security architecture zone conformance. If security zoning shown is incompatible with your organization, a zone-independent logical view is shown in figure 3.

To best illustrate a realistic alignment, some sub-zones are shown in Figure 1 and Figure 2.

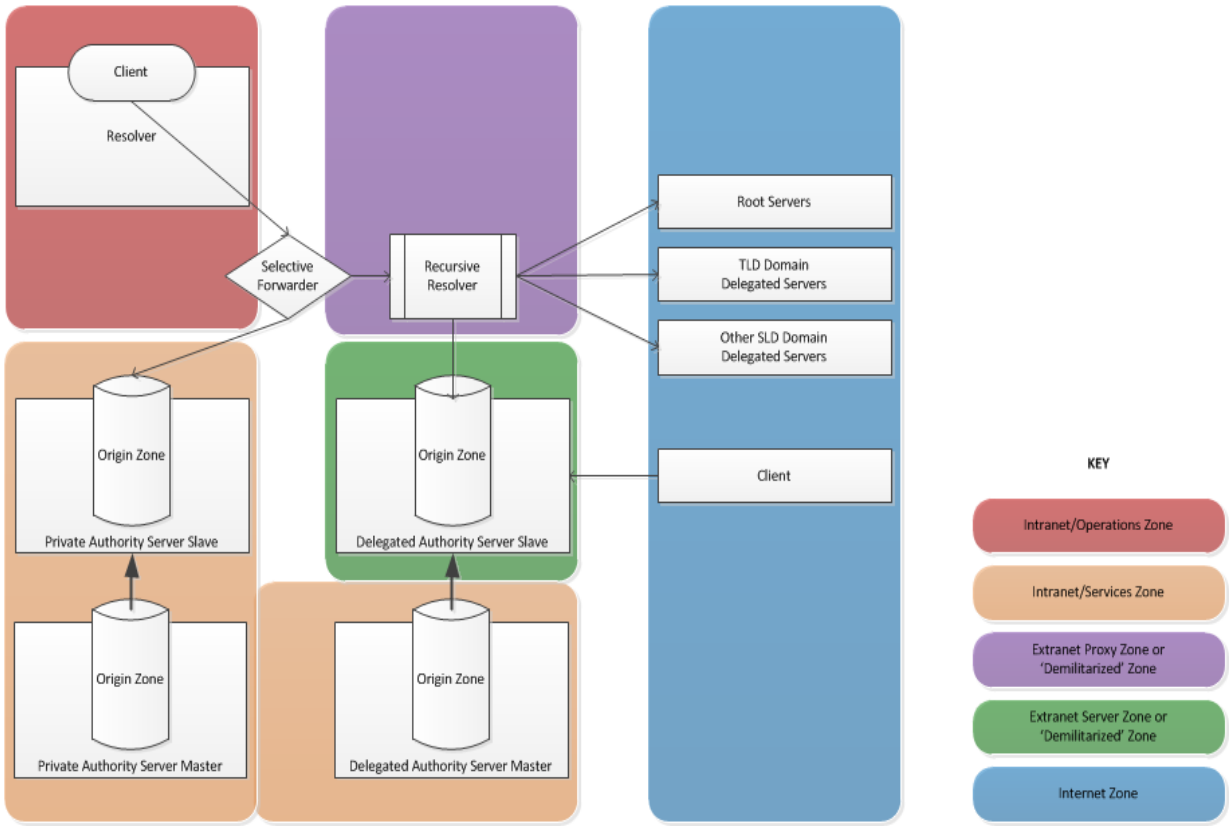

Figure 1: Representative High level Zoning for DNS

Access Network Zone

This zone hosts the network where the customer equipment (PC, phone, router) connects. It represents the "raison d'être" of the CTSP.

Customer Services Zone

This may be an enclave to the "core network" or a separate zone altogether, where general purpose server hosts offer services to the Access Network Zone. In a service provider context, this might be a service hosting zone within a centralized data center, central office, or cloud enclave where services are provided to the subscriber edge and user equipment.

Public Server Zone or "Demilitarized Zone"

This may be a network between the "public Internet" and "core network" where gateways reside, and services offered to the Internet are hosted. With increasing frequency, the implementation is virtualized into a remotely hosted "cloud" service network. For example, DNS hosting services may use this implementation model.

Public Proxy Zone or "Demilitarized Zone"

This may be a network between the "public Internet" and "core network" where gateway services allow Internet-bound sources to terminate connections. With increasing frequency, the implementation is virtualized into a remotely hosted "cloud" service network. For example, DNS filtering services may use this implementation model.

Internet "Zone"

This is typically a world-wide public IP internetwork where the organization has no specific relationship, partner or influence, but must interact and provide services to it when conducting business.

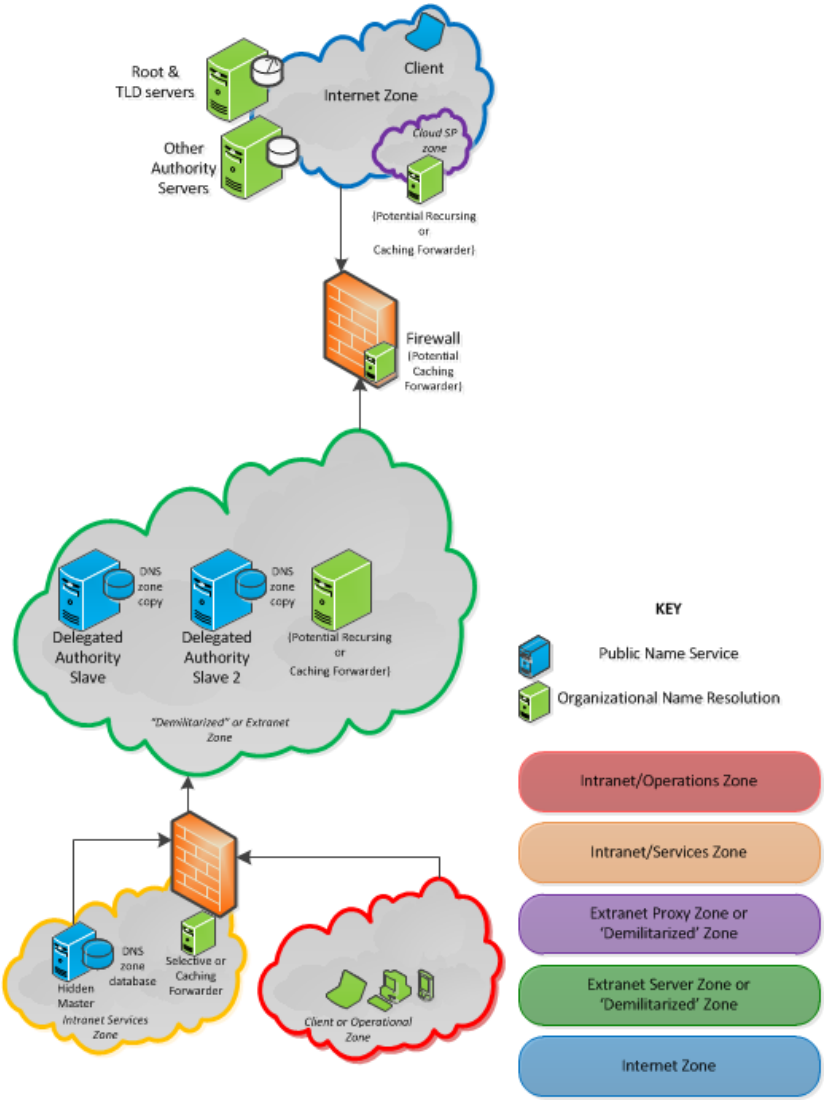

Figure 2: Network View of a Reference Architecture for as a CTSP as an Enterprise

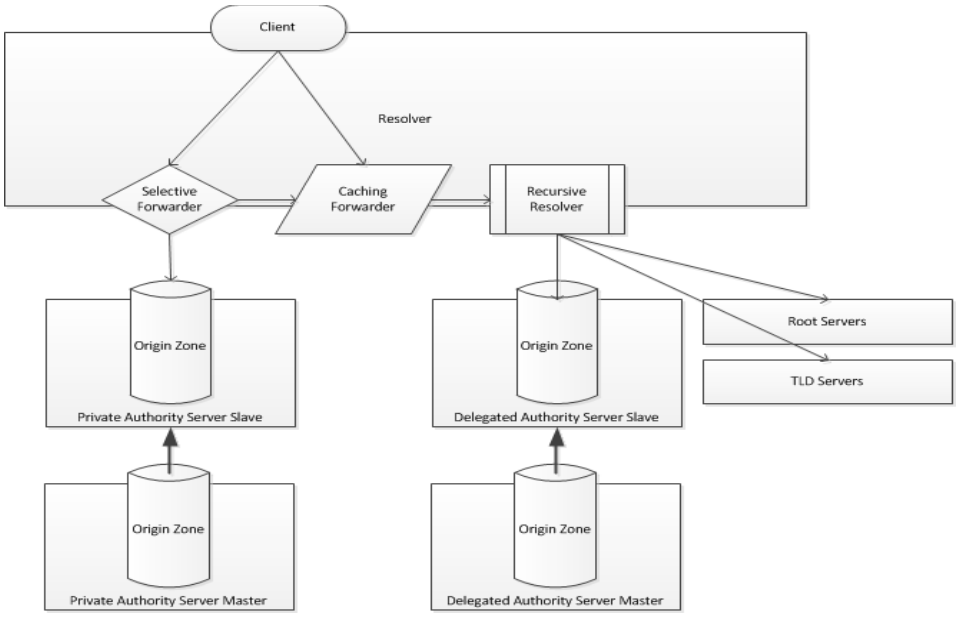

Figure 3: Symbolic View of a client resolution reference

Architecture Components

The following DNS architecture overviews indicate logical DNS components juxtaposed on a reference network zoning alignment in figure 3.

The architecture components define a target implementation for organizations seeking to implement DNS best practices, regardless of the organizations' current state. If an organization selects this reference architecture as its target design, it should then map the current implementation to this reference architecture and identify gaps between the two. This will allow an adaptive risk management process, where the organization can optimize the balance between conformance, cost, and security risk management during successive rounds of improvement. Each round of improvement would then identify, prioritize and action the closure of specific gaps between the current implementation and the desired target design.

Delegated Authority Servers

Part of the public services path, this class of component is referenced by higher order DNS servers for authoritative records about a given zone.

Public Delegated Authority Servers

Public Delegated Authority servers serve authoritative zone information that are part of the Internet DNS namespace. All other DNS servers gain knowledge about delegated authority servers through the publication of NS and SOA records which are delegated authority by higher order DNS servers. These servers hold the SOA for the authoritative

second level domain (or other strata as the case may be) and any other public facing zone.

Private Delegated Authority Servers

Private Delegated Authority servers serve authoritative zone information for “internal” or “private” namespace. This is data that the organization does not wish to serve to the public internet, providing client resolvers a different “view”. This is commonly performed in walled gardens, private enterprise networks or other closed security zones. Often multiple hosts are deployed in different geographic locations, with one master and several slaves.

Slaves

Part of the public services path, this class of component’s purpose to take a replication of the zone data from its master and serve it. The data served by a Slave may be populated via management network and specialized transport (SSH, HTTPS, etc). This practice is similar between internal and external slaves.

Public Delegated Authority Slave

The Public Delegated Authority Slave’s purpose is to take a replication of public namespace from its master and serve it to the public Internet. This data provides the Internet clients a view into public services and information. The public slave server is “delegated” because another higher-order DNS server publishes the existence of data on this server as the authority for a specific zone. A public slave may implement a zone transfer from the partner’s delegated authorities. This is primarily to enable resilience from availability issues present on a single autonomous system, BGP route, peering point, or server infrastructure. Often a reciprocal arrangement exists amongst partnered organizations on different autonomous systems and Slaves from different organizations trust one another to perform zone transfer of different zone data. In this case they are listed in a zone’s NS record.

Private Authority Slave

The Private Authority Slave’s purpose is to take a replication of internal or private namespace zone data from its master and serve it to internal or private clients. This is data that the organization does not wish to serve to the public internet, providing client resolvers a different “view” then that provided to the public Internet. This is commonly performed in walled gardens, private enterprise networks or other closed security zones. Since this slave does not typically take part in the public Internet DNS, it is not known by or delegated authority by any zones on the public Internet DNS namespace. The data served by a Slave may be populated via some management network and

specialized transport (SSH, HTTPS, etc). It does not perform secondary functions for public DNS zones.

Forwarders

Part of the resolution path, this is a class of components meant to provide resolution assistance to resolver clients to authoritative servers. These are often used to fan out scale to metro or local areas from central areas and may implement other policy functions such as compliance to a DMZ architecture that requires proxying and circuit-level termination, selectiveness, recursion or filtering.

Caching Forwarders

Caching forwarders provides an element of resilience inside an organization through caching. A caching forwarder is the most common type of forwarder one would deploy, to decrease redundant traffic volume and increase application layer resilience.

Caching Selective Forwarders

Caching selective forwarders ache and forward based on conditions in their configuration - either send to a private authoritative server or a recursive forwarder. It is caching because it remembers answers. Client resolvers ask it for names which are provided out of the forwarders cache. These are selective, because it forwards the resolution request to different upstream servers depending on the request.

Recursive Forwarder (Resolver)

Recursive forwarders talk to all Internet-facing DNS hosts directly. They can “walk” from the root servers down to the lowest level of delegation on the Internet DNS namespace to get an answer.

Areas out-of-scope include underpinning dependencies and factors beyond the reasonable control of a CTSP, such as:

1. Availability and redundancy against significant facility loss or loss due to external factors such as natural disasters;
2. Security of external physical plants and buildings; and
3. Emergency response outside of cyber issues.

Appendix B – References

These best practices leverage work done by other standards bodies referenced earlier in the document or below:

- International Organization for Standardization (ISO) 27001, 27002, 27011, 27032, and 27035;
- Communications Security Establishment Canada's (CSEC) Technology Supply Chain Guidelines for Telecommunication Equipment and Services;
- Australia's Internet Service Providers' Voluntary Code of Practice;
- Internet Engineering Task Force (IETF) Request For Comment (RFCs) including Security RFCs, Security Considerations, Ingress Filtering for Multihomed Networks.
- NIST Secure DNS Deployment Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
- Liu & Albitz. "DNS and BIND: Help for System Administrators", June 2006, O'Reilly, 5th Edition
- Anestis Karasaridis, "DNS Security: In-depth Vulnerability Analysis and Mitigation Solutions", 2 Mai 2012, Springer, édition 1
- Michael Dooley,Timothy Rooney, "DNS Security Management", Wiley-IEEE Press, july2017 Cablelabs, "Protecting ISP DNS Services from DDoS Attacks", Oct. 2016 Cablelabs, "A Vision for Secure IoT", Été 2017