DNS Privacy (dprive) Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 21, 2018

S. Bortzmeyer
AFNIC
March 20, 2018

Encryption and authentication of the DNS resolver-to-authoritative communication

draft-bortzmeyer-dprive-resolver-to-auth-01

Abstract

This document proposes a mechanism for securing (privacy-wise) the communication between the DNS resolver and the authoritative name server.

REMOVE BEFORE PUBLICATION: this document should be discussed in the IETF DPRIVE group, through its mailing list. The source of the document, as well as a list of open issues, is currently kept at Github [1].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction and background

To improve the privacy of the DNS user ([RFC7626]), the standard solution is to encrypt the requests with TLS ([RFC7858]). We use this DNS-over-TLS solution as well here, since it is standardized, already implemented in many programs, and relies on a well-known security protocol (inventing a new security protocol is quite dangerous). But just encrypting, without authenticating the remote server, leaves the user's privacy vulnerable to active man-in-the-middle attacks. [RFC7858] and [I-D.ietf-dprive-dtls-and-tls-profiles] describe how to authenticate the DNS resolver, in the stub-to-resolver link. We describe here authentication of the authoritative name server, in the resolver-to-authoritative link.

A stub DNS resolver has only a few resolvers, and there is typically a pre-existing relationship. But a resolver speaks to many authoritative name servers, without any prior relationship. This means that, for instance, having a static key for the resolver makes sense while it would be clearly unrealistic for the authoritative server.

Instead, we rely on DANE ([RFC6698]). Authoritative name servers are known by name (obtained from zone delegation). The manager of the ns1.example.net name server adds a TLSA record under example.net. The client establishes the TLS session, then authenticate in the normal DANE way.

The original charter of the DPRIVE working group, in force at the time of this draft, says "The primary focus of this Working Group is to develop mechanisms that provide confidentiality between DNS Clients and Iterative Resolvers" and adds "but it may also later consider mechanisms that provide confidentiality between Iterative Resolvers and Authoritative Servers". This document is here for this second step, "between Iterative Resolvers and Authoritative Servers". It will probably require a rechartering of the group.

2. Rules

A DNS full-service resolver who needs to query an authoritative name server establishes a TLS-over-TCP session with this authoritative name server. If the DNS material to perform DANE authentication is sent in the TLS session ([I-D.ietf-tls-dnssec-chain-extension]), it uses it. Otherwise, the resolver queries TLSA records ([RFC6698]) for this name server and authenticates the key or certificate of the server this way. If the name server is ns1.example.net, the TLSA record to query is _853._tcp.ns1.example.net.

Note that the server MAY use raw public keys ([RFC7250]) and so there is not always a certificate. If the server uses raw public keys, the TLSA record's Selector field must be 1 (SPKI, SubjectPublicKeyInfo).

The recommended order is to try TLS before querying the TLSA records. True, DANE signals if the server is willing to make DNS-over-TLS (and can therefore save a TLS attempt) but cannot guarantee that it will work (for instance if a middlebox blocks port 853). Also, the DANE records may be transferred in the TLS session, not through the DNS.

If the TLS session establishement fails, or if the DANE authentication fails, the result depends on whether the resolver runs in strict or opportunistic mode ([I-D.ietf-dprive-dtls-and-tls-profiles]). In strict mode, the resolver MUST stop using this authoritative name server, and MUST try other servers of the DNS zone. In opportunistic mode, the resolver MUST use the authoritative name server despite the failure. It MAY try other name servers of the zone before, in the hope they will accept TLS and be authenticated. To avoid a chicken-and-egg problem, the resolver, even in strict mode, MAY use unsecure servers for the meta-queries (getting the TLSA records). More specifically:

(0) The resolver remembers the keys of the authoritative name servers (in the same way it remembers the lowest RTT among an NS RRset),

(1) When the resolver needs to talk to a server (say ns2.example.net) for which it does not know the key, it does a TLSA request for _853._tcp.ns2.example.net,

(2) If the resolution of this request requires that we talk to the same server for which we're searching for the TLSA record, the resolver connects to this server with TLS to port 853, does not bother to authenticate, and sends the query. This step offers no authentication.

(See also [I-D.ietf-dprive-dtls-and-tls-profiles], section 5.) A resolver MAY use the knowledge of TLS authentication it has to choose an authoritative name server among a NS RRset.

As of this revision, we do not expect resolvers to use strict mode, since the encryption and authentication modes described in this document are not yet supported in authoritative name servers.

3. Operational considerations

DNS-over-TLS depends on TCP, and the resolver and the authoritative name server must therefore support persistent TCP connections ([RFC7766], specially section 6.2.1).

A resolver may have a lot of client-side state, when managing hundreds of connections to remote authoritative servers ([tdns]).

The latency when connecting to a authoritative name server is certainly an issue. TLS 1.3 and TCP Fast Open ([RFC7413]) may help.

Open question: do we require a minimum TLS version of 1.3? ([I-D.ietf-tls-tls13])

Because the resolver cannot know in advance if the TLS connection will work (even if there is a DANE record), using parallel attempts ("happy eyeballs", [RFC8305]) is important. A resolver working in opportunistic mode should try ports 53 and 853 in parallel.

An authoritative name server cannot know if the resolver authenticated it, nor how. In the future, it may be interesting to have an EDNS option to signal a successful authentication, or a failure, but this is out of scope currently.

If it is a concern that the same authoritative name servers are used for ordinary DNS and for encrypted DNS, there are several ways to address this concern. A server operator may use front-end systems dispatching requests to ports 53 and 853 to different servers.

A resolver must be configurable to operate in strict or opportunistic modes. Until the features described herein are widely supported, opportunistic mode should not be the default since strict mode would yield frequent failures. A resolver may have a configuration mechanism to be in strict mode only for some domains.

4. IANA Considerations

No action for IANA. This section can be deleted.

5. Security Considerations

The state to be kept in both the client and the server may make some denial-of-service attacks easier. Following the advice contained in section 10 of [RFC7766] is recommended.

In opportunistic mode, there is no guarantee to have a secure use of the DNS, or even a guarantee to be informed of a problem. Opportunistic mode is a "best effort" privacy service. Even in strict mode, some leaks may occur, through the DANE meta-queries, and through SNI indication ([I-D.ietf-tls-sni-encryption]) in the TLS session.

Neither transport encryption nor authentication protect DNS users from authentic servers which nonetheless abuse users' privacy once they've received their queries. These techniques must therefore be combined with data minimization techniques ([RFC7816]).

6. References

6.1. Normative References

[I-D.ietf-dprive-dtls-and-tls-profiles]
Dickinson, S., Gillmor, D., and T. Reddy, "Usage and (D)TLS Profiles for DNS-over-(D)TLS", draft-ietf-dprive-dtls-and-tls-profiles-11 (work in progress), September 2017.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

6.2. Informative References

[I-D.bortzmeyer-dprive-step-2]
Bortzmeyer, S., "Next step for DPRIVE: resolver-to-auth link", draft-bortzmeyer-dprive-step-2-05 (work in progress), December 2016.

[I-D.ietf-tls-dnssec-chain-extension]
Shore, M., Barnes, R., Huque, S., and W. Toorop, "A DANE Record and DNSSEC Authentication Chain Extension for TLS", draft-ietf-tls-dnssec-chain-extension-06 (work in progress), January 2018.

[I-D.ietf-tls-sni-encryption]
Huitema, C. and E. Rescorla, "SNI Encryption in TLS Through Tunneling", draft-ietf-tls-sni-encryption-02 (work in progress), March 2018.

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-27 (work in progress), March 2018.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[RFC7413] Cheng, Y., Chu, J., Radhakrishnan, S., and A. Jain, "TCP Fast Open", RFC 7413, DOI 10.17487/RFC7413, December 2014, <https://www.rfc-editor.org/info/rfc7413>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/info/rfc7626>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/info/rfc7816>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

[tdns] Liang, Z., Wessels, D., Zi, H., Heidemann, J., Mankin, A., and N. Somaiya, "T-DNS: Connection-Oriented DNS to Improve Privacy and Security; USC/ISI Technical Report ISI-TR-706", August 2014, <http://www.isi.edu/~johnh/PAPERS/Zhu16b.pdf>.

6.3. URIs

[1] https://github.com/bortzmeyer/ietf-dprive-step-2

Appendix A. Acknowledgments

Thanks to Bill Woodcock for a detailed review.

Appendix B. Alternatives

A number of other possible solutions to this problem may be found in in [I-D.bortzmeyer-dprive-step-2].

Author's Address

Stephane Bortzmeyer
AFNIC
1, rue Stephenson
Montigny-le-Bretonneux 78180
France

Phone: +33 1 39 30 83 46
Email: bortzmeyer+ietf@nic.fr
URI: http://www.afnic.fr/

dprive
Internet-Draft
Intended status: Best Current Practice
Expires: September 6, 2018

S. Dickinson
Sinodun IT
R. van Rijswijk-Deij
SURFnet bv
A. Mankin
Salesforce

March 5, 2018

Recommendations for DNS Privacy Service Operators
draft-dickinson-bcp-op-00

Abstract

This document presents operational, policy and security considerations for DNS operators who choose to offer DNS Privacy services including, but not limited to, DNS-over-TLS [RFC7858].

This document also presents a framework to assist writers of DNS Privacy Policy and Practices Statements (analogous to DNS Security Extensions (DNSSEC) Policies and DNSSEC Practice Statements described in [RFC6841]).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[NOTE: This document is submitted to the IETF for initial review and for feedback on the best forum for future versions of this document.]

The Domain Name System (DNS) was not originally designed with strong security or privacy mechanisms. [RFC7626] describes the privacy issues associated with the use of the DNS by Internet users including those related to un-encrypted DNS messages on the wire and DNS 'query log' data maintained on DNS servers.

Two documents that provide ways to increase DNS privacy between DNS clients and DNS servers are:

- Specification for DNS over Transport Layer Security (TLS) [RFC7858], referred to here as simply 'DNS-over-TLS'

- DNS over Datagram Transport Layer Security (DTLS) [RFC8094], referred to here simply as 'DNS-over-DTLS'. Note that this document has the Category of Experimental.

Both documents are limited in scope to communications between stub clients and recursive resolvers and the same scope is applied to this document. Other documents that provide further specifications related to DNS privacy include [I-D.ietf-dprive-dtls-and-tls-profiles], [RFC7830] and [I-D.ietf-dprive-padding-policy].

Note that [I-D.ietf-dnsop-dns-tcp-requirements] discusses operational requirements for DNS-over-TCP but does not provide specific guidance on DNS privacy protocols.

This document includes operational guidance related to [RFC7858] and [RFC8094].

In recent years there has been an increase in the availability of "open" resolvers. Operators of some open resolvers choose to enable protocols which encrypt DNS on the wire to cater for users who are privacy conscious. Whilst protocols that encrypt DNS messages on the wire provide protection against certain attacks, the resolver operator still has (in principle) full visibility of the query data for each user and therefore a trust relationship exists. The ability of the operator to provide a transparent, well documented, and secure privacy service will likely serve as a major differentiating factor for privacy conscious users.

More recently the global legislative landscape with regard to personal data collection, retention, and psuedo-anonymisation has seen significant activity with differing requirements active in different jurisdictions. The impact of these changes on data pertaining to the users of Internet Service Providers and specifically DNS open resolvers is not fully understood at the time of writing. It may be in certain cases that these requirement may well conflict with the IETF's end-to-end encryption principles.

This document also attempts to outline options for data handling for operators of DNS privacy services.

TODO/QUESTION: Discuss alternative (non-standard) schemes not covered by this document e.g. DNSCrypt, IPsec, VPNs. For example, should the data handling practices be recommended for any service that encrypts DNS/makes claims about DNS data privacy or is that outside the scope of this document?

This document also presents a framework to assist writers of DNS Privacy Policy and Practice Statements (DPPPS). These are documents an operator can publish outlining their operational practices and commitments with regard to privacy providing a means for clients to evaluate the privacy properties of a given DNS privacy service. In particular, the framework identifies the elements that should be considered in formulating a DPPPS. It does not, however, define a particular Policy or Practice Statement, nor does it seek to provide legal advice or recommendations as to the contents.

Community knowledge about operational practices can change quickly, and experience shows that a Best Current Practice (BCP) document about privacy and security is a point-in-time statement. Readers are advised to seek out any errata or updates that apply to this document.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC8174].

- o Privacy-enabling DNS server: A DNS server that implements DNS-over-TLS [RFC7858] and may optionally implement DNS-over-DTLS [RFC8094]. The server should also offer at least one of the credentials described in Section 8 of [I-D.ietf-dprive-dtls-and-tls-profiles] and implement the (D)TLS profile described in Section 9 of [I-D.ietf-dprive-dtls-and-tls-profiles].

- o DPPPS: DNS Privacy Policy and Practice Statement, see Section 6.

- o DNS privacy service: The service that is offered via a privacy-enabling DNS server and is documented either in an informal statement of policy and practice with regard to users privacy or a formal DPPPS.

3. Server capabilities to maximise DNS privacy

3.1. General capabilities

In addition to Sections 9 and 11.1 of [I-D.ietf-dprive-dtls-and-tls-profiles] DNS privacy services SHOULD offer the following capabilities/options:

- QNAME minimisation [RFC7816]
- Management of TLS connections to optimise performance for clients using either
  * [RFC7766] and EDNS(0) Keepalive [RFC7828] and/or
  * DNS Stateful Operations [I-D.ietf-dnsop-session-signal]
- No requirement that clients must use TLS session resumption [RFC5077] (or Domain Name System (DNS) Cookies [RFC7873])

DNS privacy services MAY offer the following capabilities:

- DNS privacy service on both port 853 and 443 (to circumvent blocking of port 853)
- A .onion [RFC7686] service endpoint
- Aggressive Use of DNSSEC-Validated Cache [RFC8198] to reduce the number of queries to authoritative servers to increase privacy.
- Run a copy of the root zone on loopback [RFC7706] to avoid making queries to the root servers that might leak information.

QUESTION: Should we say anything here about filtering responses or DNSSEC validation e.g. operators SHOULD provide an unfiltered service on an alternative IP address if the 'main' DNS privacy address filters responses? Or simply just to say that the DNS privacy service should not differ from the 'normal' DNS service in terms of such options.

3.2. Client query obfuscation

Since queries from recursive resolvers to authoritative servers are performed using cleartext (at the time of writing), resolver services need to consider the extent to which they may be directly leaking information about their client community via these upstream queries and what they can do to mitigate this further. Note, that even when all the relevant techniques described above are employed there may still be attacks possible, e.g. [Pitfalls-of-DNS-Encryption]. For example, a resolver with a very small community of users risks exposing data in this way and MAY want to obfuscate this traffic by mixing it with 'generated' traffic to make client characterisation harder.

3.3. Availability

As a general model of trust between users and service providers DNS privacy services should have high availability. Denying access to an encrypted protocol for DNS queries forces the user to switch providers, fallback to cleartext or accept no DNS service for the outage.

3.4. Authentication of DNS privacy services

To enable users to select a 'Strict Privacy' usage profile [I-D.ietf-dprive-dtls-and-tls-profiles] DNS privacy services should provide credentials in the form of either X.509 certificates, SPKI pinsets or TLSA records. This in effect commits the DNS privacy service to a public identity users will trust.

Anecdotal evidence to date highlights this requirement as one of the more challenging aspects of running a DNS privacy service as management of such credentials is new to DNS operators.

3.4.1. Generation and publication of certificates

It is RECOMMENDED that operators:

- o Choose a short, memorable authentication name for their service

- o Automate the generation and publication of certificates

- o Monitor certificates to prevent accidental expiration of certificates

3.4.2. Management of SPKI pins

TODO

3.4.3. TLSA records

TODO

4. Operational management

4.1. Limitations of using a pure TLS proxy

Some operators may choose to implement DNS-over-TLS using a TLS proxy (e.g. nginx [1] or haproxy [2]) in front of a DNS nameserver because of proven robustness and capacity when handling large numbers of client connections, load balancing capabilities and good tooling. Currently, however, because such proxies typically have no specific handling of DNS as a protocol over TLS or DTLS using them can restrict traffic management at the proxy layer and at the DNS server. For example, all traffic received by a nameserver behind such a proxy will appear to originate from the proxy and DNS techniques such as ACLs or RRL will be hard or impossible to implement in the nameserver.

4.2. Anycast deployments

TODO:

5. Server data handling

The following are common activities for DNS service operators and in all cases should be minimised or completely avoided if possible for DNS privacy services. If data is retained it should be encrypted and either aggregated, psuedo-anonymised or de-identified whenever possible.

- o Logging and Monitoring: Only that required to sustain operation of the service and meet regulatory requirements.

- o Data retention: Data SHOULD be retained for the shortest period deemed operationally feasible.

- o User tracking: DNS privacy services SHOULD not track users. An exception may be malicious or anomalous use of the service.

- o Providing data to third-parties (sharing, selling or renting): Operators SHOULD not provide data to third-parties without explicit consent from users (simply using the resolution service itself does not constitute consent).

- o Access to stored personal data: Access SHOULD be minimised to only those personal who require access to perform operational duties.

5.1. Psuedo-anonymisation and de-identification methods

There is active discussion in the space of effective psuedo-anonymisation of personal data in DNS query logs. To-date this has focussed on psuedo-anonymisation of client IP addresses, however there are as yet no standards for this that are unencumbered by patents. This section briefly references some know methods in this space at the time of writing.

5.1.1. ipcipher

[ipcipher-spec] is a psuedo-anonymisation technique which encrypts IPv4 and IPv6 addresses such that any address encrypts to a valid address. At the time of writing the specification is under review and may be the subject of a future IETF draft.

5.1.2. Bloom filters

There is also on-going work in the area of using Bloom filters as a privacy-enhancing technology for DNS monitoring [DNS-bloom-filter]. The goal of this work is to allow operators to identify so-called Indicators of Compromise (IOCs) originating from specific subnets without storing information about, or be able to monitor the DNS queries of an individual user.

6. DNS privacy policy and practice statement

6.1. Current privacy statements

TODO: Compare main elements of Google vs Quad9 vs OpenDNS policies

6.2. Recommended contents of a DPPPS

- o Policy: This section should explain the policy for gathering and disseminating information collected by the DNS privacy service.

  - * Specify clearly what data (including whether it is aggregated, psuedo-anonymised or de-identified) is

  - * Collected and retained by the operator (and for how long)

  - * Shared with, sold or rented to third-parties

  - * Specify any exceptions to the above, for example malicious or anomalous behaviour

  - * Declare any third-party affiliations or funding

  * Whether user DNS data is correlated or combined with any other personal information held by the operator

- Practice: This section should explain the current operational practices of the service.

  * Specify any temporary or permanent deviations from the policy for operational reasons

  * Provide specific details of which capabilities are provided on which address and ports

  * Specify the authentication name to be used (if any)

  * Specify the SPKI pinsets to be used (if any) and policy for rolling keys

  * Provide a contact email address for the service

6.3. Enforcement/accountability

Transparency reports may help with building user trust that operators adhere to their policies and practices.

Independent monitoring should be performed where possible of:

- ECS, QNAME minimisation, EDNS(0) padding, etc.

- Filtering

- Uptime

7. IANA considerations

None

8. Security considerations

TODO: e.g. New issues for DoS defence, server admin policies

9. Acknowledgements

Many thanks to John Dickinson for review of and input to the first draft of this document.

Thanks to Benno Overeinder and John Todd for discussions on this topic.

10. Changelog

draft-dickinson-dprive-bcp-op-00

- Initial commit

11. References

11.1. Normative References

[I-D.ietf-dnsop-session-signal]
Bellis, R., Cheshire, S., Dickinson, J., Dickinson, S., Mankin, A., and T. Pusateri, "DNS Stateful Operations", draft-ietf-dnsop-session-signal-05 (work in progress), January 2018.

[I-D.ietf-dprive-dtls-and-tls-profiles]
Dickinson, S., Gillmor, D., and T. Reddy, "Usage and (D)TLS Profiles for DNS-over-(D)TLS", draft-ietf-dprive-dtls-and-tls-profiles-11 (work in progress), September 2017.

[I-D.ietf-dprive-padding-policy]
Mayrhofer, A., "Padding Policy for EDNS(0)", draft-ietf-dprive-padding-policy-04 (work in progress), February 2018.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <https://www.rfc-editor.org/info/rfc5077>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/info/rfc7626>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/info/rfc7816>.

[RFC7828] Wouters, P., Abley, J., Dickinson, S., and R. Bellis, "The edns-tcp-keepalive EDNS0 Option", RFC 7828, DOI 10.17487/RFC7828, April 2016, <https://www.rfc-editor.org/info/rfc7828>.

[RFC7830] Mayrhofer, A., "The EDNS(0) Padding Option", RFC 7830, DOI 10.17487/RFC7830, May 2016, <https://www.rfc-editor.org/info/rfc7830>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

[DNS-bloom-filter] van Rijswijk-Deij, R., Bomhoff, M., and R. Dolmans, "Let a Thousand Filters Bloom. DNS-Based Threat Monitoring That Respects User Privacy", 2018, < https://tnc18.geant.org/getfile/3823>.

[I-D.ietf-dnsop-dns-tcp-requirements] Kristoff, J. and D. Wessels, "DNS Transport over TCP - Operational Requirements", draft-ietf-dnsop-dns-tcp-requirements-01 (work in progress), November 2017.

[ipcipher-spec] Hubert, B., "ipcipher: encrypting IP addresses", 2018, <https://powerdns.org/ipcipher/>.

[Pitfalls-of-DNS-Encryption] Shulman, H., "Pretty Bad Privacy: Pitfalls of DNS Encryption", 2014, <https://www.ietf.org/mail-archive/web/dns-privacy/current/pdfWqAIUmEl47.pdf>.

[RFC6841] Ljunggren, F., Eklund Lowinder, AM., and T. Okubo, "A Framework for DNSSEC Policies and DNSSEC Practice Statements", RFC 6841, DOI 10.17487/RFC6841, January 2013, <https://www.rfc-editor.org/info/rfc6841>.

[RFC7686] Appelbaum, J. and A. Muffett, "The ".onion" Special-Use Domain Name", RFC 7686, DOI 10.17487/RFC7686, October 2015, <https://www.rfc-editor.org/info/rfc7686>.

[RFC7706] Kumari, W. and P. Hoffman, "Decreasing Access Time to Root Servers by Running One on Loopback", RFC 7706, DOI 10.17487/RFC7706, November 2015, <https://www.rfc-editor.org/info/rfc7706>.

[RFC8198] Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198, July 2017, <https://www.rfc-editor.org/info/rfc8198>.

11.3. URIs

[1] https://nginx.org/

[2] https://www.haproxy.org/

Authors' Addresses

Sara Dickinson
Sinodun IT
Magdalen Centre
Oxford Science Park
Oxford OX4 4GA
United Kingdom

Email: sara@sinodun.com

Roland M. van Rijswijk-Deij
SURFnet bv
PO Box 19035
Utrecht 3501 DA Utrecht
The Netherlands

Email: roland.vanrijswijk@surfnet.nl

Allison Mankin
Salesforce

Email: allison.mankin@gmail.com