

Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 10, 2015

A. Mohaisen
A. Mankin
Verisign Labs
March 9, 2015

Evaluation of Privacy for DNS Private Exchange
draft-am-dprive-eval-00

Abstract

The set of DNS requests that an individual makes can provide an attacker with a large amount of information about that individual. DNS Private Exchange (DPRIVE) aims to deprive the attacker of this information. This document describes methods for measuring the performance of DNS privacy mechanisms, particularly it provides methods for measuring effectiveness in the face of pervasive monitoring as defined in [RFC7258](#). The document includes example evaluations for common use cases.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 10, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Motivation	3
2.	Privacy Evaluation Definitions	5
2.1.	RFC 6973 Definitions - Entities	5
2.2.	RFC 6973 Definitions - Data and Analysis	6
2.3.	RFC 6973 Definitions - Identifiability	7
2.4.	Other Central Definitions and Formalizations	8
3.	Assumptions about Quantification of Privacy	10
4.	System Model	11
4.1.	DNS Resolvers (System Model)	11
4.2.	System Setup - Putting It Together	11
5.	Attack Model	14
5.1.	Attacker Type-1 - Pervasive Monitor	14
5.2.	Attacker Type-2 - Malicious Monitor	14
5.3.	Attackers in the System Setup	15
6.	Privacy Mechanisms	16
7.	Privacy Evaluation	18
8.	Security Considerations	23
9.	IANA Considerations	24
10.	Acknowledgements	25
11.	Informative References	26
	Authors' Addresses	28

1. Motivation

One of the IETF's core views is that protocols should be designed to enable security and privacy while online [[RFC3552](#)]. In light of the recent reported pervasive monitoring efforts, another goal is to design protocols and mechanisms to make such monitoring expensive or infeasible to conduct. As detailed in the DPRIVE problem statement [[dprive-problem](#)], DNS resolution is an important arena for pervasive monitoring, and in some cases may be used for breaching the privacy of individuals. The set of DNS requests that an individual makes can provide a large amount of information about that individual. Not only individual requesters reveal information with their sets of DNS queries. In some specific use cases, the sets of DNS requests from a DNS recursive resolver or other entity may also provide revealing information. This document describes methods for measuring the performance of DNS privacy mechanisms; in particular, it provides methods for measuring effectiveness in the face of pervasive monitoring as defined in [[RFC7258](#)]. The document includes example evaluations for common use cases.

The privacy risks associated with DNS monitoring are not new, however they were brought into a greater visibility by the issue described in [[RFC7258](#)]. The DPRIVE working group was formed to respond and at this time has several DNS private exchange mechanisms in consideration, including [[dns-over-tls](#)], [[confidential-dns](#)], [[phb-dnse](#)], and [[privatedns](#)]. There is also related work in other working groups, including DNSOP: [[qname-minimisation](#)] and (potentially) DANE [[ipseca](#)]. The recently published [[RFC7435](#)] also has relevance to DNS private exchange.

Each effort related to DNS privacy mechanisms asserts some privacy assurances and operational relevance. Metrics for these privacy assurances are needed and are in reach based on existing techniques from the general field of privacy engineering. Systematic evaluation of DNS privacy mechanisms will enhance the likely operational effectiveness of DNS private exchange.

Evaluating an individual mechanism for DNS privacy could be accomplished on a one-off basis, presumably as Privacy Considerations within each specification, but this will not address as much variation of operational contexts nor will it cover using multiple mechanisms together (in composition). [Section 2 of \[RFC6973\]](#) discussed both benefits and risks of using multiple mechanisms.

Definitions required for evaluating the privacy of stand-alone and composed design are not limited to privacy notions, but also need to include the attacker model and some information about relationships among the entities in a given system. A mechanism for providing

privacy to withstand the power and capabilities of a passive pervasive monitor may not withstand a more powerful attacker using active monitoring by plugging itself into the path of individuals' DNS requests as a forwarder, or worse, by controlling a DNS recursive server (that is, in what we define later as the malicious attack model). Having some standard attack models, and understanding how applicable they are to various designs is a part of evaluating the privacy.

Sections [2](#) and [3](#) present privacy terminology and some assumptions. Sections [4](#) and [5](#) cover the system model or setup and the attack models. In [Section 6](#), we review a list of DNS privacy mechanisms, including some which are not in scope of the DPRIVE working group. [Section 7](#) tackles how to evaluate privacy mechanisms, in the form of templates and outcomes. Given a specific attack model, the guarantees with respect to privacy of an individual or an item of interest are quantified.

[2.](#) Privacy Evaluation Definitions

This section provides definitions to be used for privacy evaluation of DNS. [\[RFC6973\]](#) is the verbatim source of most of the definitions. Text is added to apply them to the DNS case. We follow the [\[RFC6973\]](#) in classifying the terms. We have added a new section of terms to include several important practical or conventional terms that were not included in [\[RFC6973\]](#) such as PII. For the terms from [\[RFC6973\]](#), we include their definitions rather than simply referencing them as an aid to readability.

[2.1.](#) [RFC 6973](#) Definitions - Entities

- o Attacker: An entity that works against one or more privacy protection goals. Unlike observers, attackers' behavior is unauthorized.
- o Eavesdropper: A type of attacker that passively observes an initiator's communications without the initiator's knowledge or authorization. This may include a passive pervasive monitor, defined below.

- o Enabler: A protocol entity that facilitates communication between an initiator and a recipient without being directly in the communications path. DNS examples of an enabler in this sense include a recursive resolver, a proxy, or a forwarder.
- o Individual: A human being (or a group of them)
- o Initiator: A protocol entity that initiates communications with a recipient.
- o Intermediary: A protocol entity that sits between the initiator (stub resolver) and the recipient (recursive resolver or authority resolver) and is necessary for the initiator and recipient to communicate. Unlike an eavesdropper, an intermediary is an entity that is part of the communication architecture and therefore at least tacitly authorized.
- o Observer: An entity that is able to observe and collect information from communications, potentially posing privacy threats, depending on the context. As defined in this document, initiators, recipients, intermediaries, and enablers can all be observers. Observers are distinguished from eavesdroppers by being at least tacitly authorized.

[2.2. RFC 6973](#) Definitions – Data and Analysis

- o Attack: An intentional act by which an entity attempts to violate an individual's privacy. See [\[RFC4949\]](#).
- o Correlation: The combination of various pieces of information that relate to an individual or subject, or that obtain that characteristic when combined.
- o Fingerprint: A set of information elements that identifies a device or application instance.
- o Fingerprinting: The process of an observer or attacker uniquely identifying (with a sufficiently high probability) a device or application instance based on multiple information elements

communicated to the observer or attacker. See [EFF].

- o Item of Interest (IOI): Any data item that an observer or attacker might be interested in. This includes attributes, identifiers, identities, communications content, and the fact that a communication interaction has taken place. In the DNS private exchange context, items of interest can be Source IP address, ASN of the Source IP address, and the query itself, including the qname, and other attributes.
- o Personal Data: Any information relating to an individual who can be identified, directly or indirectly. Note that when a Subject is involved that is not an individual, we will identify Items of Interest but not reference this as Personal.
- o (Protocol) Interaction: A unit of communication within a particular protocol. A single interaction may be comprised of a single message between an initiator and recipient or multiple messages, depending on the protocol.
- o Traffic Analysis: The inference of information from observation of traffic flows (presence, absence, amount, direction, timing, packet size, packet composition, and/or frequency), even if flows are encrypted. See [\[RFC4949\]](#).
- o Undetectability: The inability of an observer or attacker to sufficiently distinguish whether an item of interest exists or not.
- o Unlinkability: Within a particular set of information, the inability of an observer or attacker to distinguish whether two items of interest are related or not (with a high enough degree of probability to be useful to the observer or attacker).

[2.3.](#) [RFC 6973](#) Definitions - Identifiability

- o Anonymity: The state of being anonymous.
- o Anonymity Set: A set of individuals that have the same attributes, making them indistinguishable from each other from the perspective of a particular attacker or observer.

- o Anonymous: A state of an individual in which an observer or attacker cannot identify the individual within a set of other individuals (the anonymity set).
- o Attribute: A property of an individual or subject.
- o Identifiability: The extent to which an individual is identifiable. [\[RFC6973\]](#) has the rest of the variations on this (Identifiable, Identification, Identified, Identifier, Identity, Identity Confidentiality)
- o Identity Provider: An entity (usually an organization) that is responsible for establishing, maintaining, securing, and vouching for the identities associated with individuals.
- o Personal Name: A natural name for an individual. Personal names are often not unique and often comprise given names in combination with a family name. An individual may have multiple personal names at any time and over a lifetime, including official names. From a technological perspective, it cannot always be determined whether a given reference to an individual is, or is based upon, the individual's personal name(s) (see Pseudonym). NOTE: The reason to import this definition is that some query names that cause privacy leakage do so by embedding personal names as identifiers of host or other equipment, e.g. AllisonMankinMac.example.com.
- o Pseudonymity: See the formal definition in the next section in lieu of [\[RFC6973\]](#).

NOTE: Identifiability Definitions in [\[RFC6973\]](#) also include some material not included here because the distinctions are not major for DNS Private Exchange, such as real and official names, and variant forms of Pseudonymity in its informal definition.

Relying Party: An entity that relies on assertions of individuals' identities from identity providers in order to provide services to individuals. In effect, the relying party delegates aspects of identity management to the identity provider(s). Such delegation requires protocol exchanges, trust, and a common understanding of

the identity provider.

[2.4.](#) Other Central Definitions and Formalizations

Central to the presentation of this document is the definition of personally identifiable information (PII), as well as other definitions that supplement the definitions listed earlier. In this section, we outline such definitions we further notes on their indications.

- o Personally Identifiable Information (PII): Information (attributes) that can be used as is, or along with other side information, to identify, locate, and/or contact a single individual or subject (c.f. item of interest).

NOTE: the definition above indicates that PII can be used on its own or in context. In DNS privacy, the items without additional context include IP(v4 or v6) address, qname, qtype, timings of queries, etc. The additional context includes organization-level attributes, such as a network prefix that can be associated with an organization. The definition of PII is complementary to the definition of items of interest.

- o Subject: This term is useful as a parallel term to Individual. When the privacy of a group or an organization is of interest to an attacker, we can reference the group or organization as Subject rather than Individual.

Often it is desirable to reference alternative identifiers known as pseudonyms. A pseudonym is a name assumed by an individual in some context, unrelated to the names or identifiers known by others in that context.

- o Pseudonymity/Pseudonym: a relaxation of the definition of anonymity for usability. In particular, pseudonymity is an anonymity feature obtained by using a pseudonym, an identifier that is used for establishing a long relationship between two entities.

As an example, in the DNS context, a randomly generated pseudonym might identify a set of query data with a shared context, such as geographic origin. Such pseudonymity enables another entity or attacker to link multiple queries on a long-term basis. Pseudonyms are assumed long-lived and their uniqueness may be a goal. There are many findings that indicate that pseudonymity is weaker than anonymity.

- o Unlinkability: Formally, two items of interest are said to be unlinkable if the certainty of the attacker concerning those items of interest is not affected by observing the system. This is, unlinkability implies that the a-posteriori probability computed by the attacker that two items of interest are related is close enough to the a-priori probability computed by an attacker based on his knowledge.

Two items of interest are said to be unlinkable if there is a small (beta, close to 0) probability that the attacker identifies them as associated, and they are linkable if there is a sufficiently large probability (referred to as alpha).

Informally, given two items of interest (user attributes, DNS queries, users, etc.), unlinkability is defined as the inability of the attacker to sufficiently determine whether those items are related to one another. In the context of DNS, this refers typically but not only to an attacker relating queries to the same individual.

- o Undetectability: a stronger definition of privacy, where an item of interest is said to be undetectable if the attacker is not sufficiently able to know or tell whether the item exists or not.

Note that undetectability implies unlinkability. As explained below, a way of ensuring undetectability is to use encryption secure under known ciphertext attacks, or randomized encryption.

- o Unobservability: a stronger definition of privacy that requires satisfying both undetectability and anonymity. Unobservability means that an item of interest is undetectable by any uninvolved individual, attacker or not.

In theory, there are many ways of ensuring unobservability by fulfilling both requirements. For example, undetectability requires that no party uninvolved in the resolution of a DNS query shall know that query has existed or not. A mechanism to ensure this function is encryption secure under known ciphertext attacks, or randomized encryption for all other than stub, and pseudonyms for the stub resolver. An alternative mechanism to provide the anonymity property would be the use of mix networks for routing DNS queries.

[3.](#) Assumptions about Quantification of Privacy

The quantification of privacy is connected with the privacy goals. Is the desired privacy property unlinkability only, or is it undetectability. Is pseudonymity a sufficient property? Parameters and entire privacy mechanism choices are affected by the choice of privacy goals.

While a binary measure of privacy is sometimes possible, that is, being able to say that the transaction is anonymous, in this document, we assume that the binary is not frequently obtainable, and therefore we focus on methods for continuous quantification. Both are relevant to DNS Private Exchange. Another way to state this is that the quantification could be exactly the probabilities 1 and 0, corresponding to the binary, but the methods prefer to provide continuous values instead.

Here is an example of continuous quantification, related to identifiability of an individual or item of interest based on observing queries.

- o For an individual A , and a set of observations by an attacker, $Y = [y_1, y_2, \dots, y_n]$, we define the privacy of A as the uncertainty of the attacker of knowing that A is itself among many others under the observations Y ; that is, we define $\text{Privacy} = 1 - P[A \mid Y]$
- o For an item of interest r associated with a user A , we similarly define the privacy of r as $\text{Privacy} = 1 - P[r \mid Y]$.

[4.](#) System Model

A DNS client (a DNS stub resolver) may resolve a domain name or address into the corresponding DNS record by contacting the authoritative name server responsible for that domain name (or address) directly. However, to improve the operation of DNS resolution, and reduce the round trip time required for resolving an address, both caching and recursive resolution are implemented. Caching is implemented at an intermediary between the stub and the authoritative name server. In practice, many caching servers also implement the recursive logic of DNS resolution for finding the name server authoritative for a domain, and are thus named DNS recursive resolvers. Another type of entity, forwarders (or proxies) are intermediaries between the three named here. The system model for DNS privacy evaluation includes the four entities quickly sketched here: stub resolvers, recursive resolvers, authoritative name servers, and forwarders.

[4.1.](#) DNS Resolvers (System Model)

- o Stub resolver (S): a minimal resolver that does not support referral, and delegates recursive resolution to a recursive resolver. A stub resolver is a consumer of recursive resolutions. Per the terminology of [[RFC6973](#)], a stub resolver is an Initiator.
- o Recursive resolver (R): a resolver that implements the recursive function of DNS resolution on behalf of a stub resolver. Per the terminology of [[RFC6973](#)], a recursive resolver is an Enabler.
- o Authoritative resolver (A): is a server that is the origin of a DNS record. A recursive resolver queries the authoritative resolver to resolve a domain name or address. Per the terminology

of [[RFC6973](#)], the authoritative name server is also an Enabler.

- o Forwarder/proxy (P): between the stub resolver and the authoritative resolver there may be more than one DNS-involved entity. These are systems located between S and R (stub resolver and recursive), or between R and A (recursive and authoritative), which do not play a primary role in the DNS protocol. Per the terminology of [[RFC6973](#)], forwarders are Intermediaries.

[4.2.](#) System Setup - Putting It Together

Evaluating various privacy protection mechanisms in relation to attackers such as the pervasive monitoring attackers defined next requires understanding links in the System setup. We define the following links. In relation to [[RFC7258](#)] these are the attack surface where a monitor (eavesdropper) collects sets of query

Mohaisen & Mankin	Expires September 10, 2015	[Page 11]
-------------------	----------------------------	-----------

Internet-Draft	Evaluation of Privacy for DNS	March 2015
----------------	-------------------------------	------------

information.

- o Stub -> Recursive (S-R): a link between the stub resolver and a recursive resolver. At the time of writing, the scope of DPRIVE Working Group privacy mechanisms is supposed to be limited to S-R.
- o Stub -> Proxy (S-P): a link between the stub resolver and a forwarder/ proxy. The intended function of this link may be difficult to analyze.
- o Proxy -> Recursive (P-R): a link between a proxy and a recursive server.
- o Recursive -> Authoritative (R-A): a link between a recursive and an authoritative name server. Although at the time of writing, R-A is not in the DPRIVE scope, we touch on it in evaluations.

Rather than notating in system setup that an entity is compromised, this is covered in the attacker model in [Section 6](#), which has system elements as parameters.

In the System Setup, there is a possibility that S and R exist on a single machine. The concept of the Unlucky Few relates S and R in this case. An attacker can monitor R-A and find the query traffic of the initiator individual. The same concept applies in the case where

a recursive is serving a relatively small number of individuals. The query traffic of a subject group or organization (c.f. Subject in the definitions) is obtained by the attacker who monitors this system's R-A.

Because R-A is not in the DPRIVE scope, it is for future work to examine the Unlucky Few circumstance fully. The general system setup is that PII, the individual's private identifying information, is not sent on R-A and is not seen by authoritatives.

There could be one or more proxies between the stub resolver and a recursive. From a functionality point of view they can all be consolidated into a single proxy without affecting the system view, however, the behavior of such proxies may affect the size and shape of the attack surface. However, we believe that an additional treatment is needed for this case and it is not included in the discussion.

We also do not include in discussion proxies that exist along R-A, between a recursive and an authoritative name server. We do so in respect for the DPRIVE charter's scope at this time. According to recent work at [openresolverproject.org], there may be multiple intermediaries with poorly defined behavior.

The system setup here leaves out other realistic considerations for simplicity, such as the impact of shared caches in DNS entities.

[5.](#) Attack Model

The Definitions section defines Attack and Attacker, but not Attack Model, which is needed to actually evaluate privacy, so this is now defined.

- o Attack Model: a well-defined set of capabilities indicating how much information the attacker has and in what context in order to reach a goal of breaching the privacy of an individual or subject with respect to a given privacy metric.

In this document we focus on two attack models, namely a pervasive monitor and a malicious monitor. The first attack model has two forms, namely active and passive attack models, which are defined in the following.

5.1. Attacker Type-1 - Pervasive Monitor

This attacker corresponds to the pervasive monitoring adversary described in [RFC7258]. This attacker relies on monitoring capabilities to breach the privacy of individuals from the DNS traffic. This attacker is capable of eavesdropping on traffic between two end points, including traffic between any of the pairs of the entities described in [section 2.1](#). Per [RFC7258], this type of attacker has abilities to eavesdrop pervasively on many links at once, which is a powerful form of attack. Type-1 Attackers are passive. They do not modify traffic or insert traffic.

- o Type-1A: Pervasive Monitor: an attacker who is able to monitor links carrying individual's traffic through access to traffic along those links. This attacker does not specifically target the links of a particular individual. This attacker uses its system location to launch attacks and learn as much as possible about all individuals using those links.
- o Type-1B: Directed Monitor: an attacker with the same types of capabilities of monitoring links, which selects links in order to target specific individuals. A Type-1B attacker for instance might put into place intermediaries in order to obtain traffic on specific links.

5.2. Attacker Type-2 - Malicious Monitor

This attacker is more powerful than Type-1. It corresponds to the malicious attack model that is widely studied in the security community. Formally, an attacker in the malicious monitor model has all of the active pervasive monitor capabilities as well as the capability to control one or more infrastructure elements, to modify

traffic in both directions. This type of attacker could have a malicious recursive server or forwarder under its control, for example.

[5.3.](#) Attackers in the System Setup

To evaluate the privacy provided by a given mechanism or mechanisms in a particular system model, we characterize the attacker with a template with parameters from the system model in which the attacker is located. The general template is: `Attacker(Type, [Compromised_Entities], [Links])`. For example, the template `Attacker(Type-2, R, S-R)` passed as a parameter in the evaluation of a privacy mechanism indicates a Type-2 attacker that controls a recursive and has the capability of eavesdropping on the link between the stub and recursive resolvers. Other attacker templates include the appropriate parameterizations based on the above description of those attackers, including attackers that have the capabilities of monitoring multiple links and controlling multiple pieces of infrastructure.

6. Privacy Mechanisms

Various mechanisms for enhancing privacy in networks are applicable to DNS private exchange. Some mechanisms common to privacy research include mixing networks, dummy traffic, and private information retrieval techniques. Applicable protocol mechanisms include encryption-based techniques - encrypting the channel carrying the queries using IPSEC [[ipseca](#)], TLS [[dns-over-tls](#)] or special-purpose encryption [[confidential-dns](#)]. [[privatedns](#)] includes special-purpose encryption and also depends on a trusted service broker.

- o **Mixing Networks:** in this type of mechanism, the initiator uses a mixing network such as Tor to route the DNS queries to the intended DNS server entity. An attacker observing part of the system finds it difficult to determine which individual sends which queries, and will not be able to tell which individual has sent them (ideally, though it is known that attacks exist that allow correlation and privacy breaches against mixing networks). The privacy property is unlinkability of the queries; the probability that two queries coming from one exit node in the mixing network belong to the same individual is uniform among all the individuals using the network.
- o **Dummy Traffic:** a simple mechanism in which the initiator of a DNS request will also generate k dummy queries and send the intended query along with those queries. As such, the adversary will not be able to tell which query is of interest to the initiator. For a given k , the probability that the adversary will be able to detect which query is interest to the initiator is equal to $1/(k+1)$. In that sense, and for the proper parameterization of the protocol, the attacker is bounded to the undetectability of the queries.
- o **Private Information Retrieval:** a mechanism that allows a user s to retrieve a record r from a database DB on a server without allowing the server to learn r . A trivial solution to the problem requires that s downloads the entire DB and then perform the queries locally. While that provides privacy to the queries of the user, the solution is communication inefficient at the scale of the DNS. More sophisticated cryptographic solutions are multi-round, and thus reduce the communication overhead, but are still inefficient for the DNS.
- o **Query Minimization:** a mechanism that allows the resolver to minimize the amount of information it sends on behalf of a stub resolver. A method of query minimization is specified in [[qname-minimisation](#)]. Qname minimization deprives a Type-1

attacker on R-A of information from correlating queries, unless

the individuals have an Unfortunate Few problem.

- o NOTE: queries on R-A generally do not include an identifier of the individual making the query, because the source address is that of R. With respect R or A themselves, they may have well established policies for respecting the sensitivity of queries they process, while still using summary analysis of those queries to improve security, stability or their business operation.
- o Encrypted Channel Mechanisms: Using these mechanisms, an initiator has an encrypted channel with a corresponding enabler, so that the queries are not available to eavesdropping Pervasive Monitor attackers. Examples include [[dns-over-tls](#)], [[ipseca](#)], and [[confidential-dns](#)]. Depending on the characteristics of the channel, various privacy properties are ensured. For instance, undetectability of queries is ensured for encryption-based mechanisms once the encrypted channel is established. Unlinkability of the queries may depend on the type of crypto-suite; it is provided as long as randomized encryption is used.
- o Composed (Multiple) Mechanisms: the use of multiple mechanisms is a likely scenario and results in varied privacy guarantees. Consider a hypothetical system in which mixing networks (for unlinkability) and randomized encryption (for undetectability) can both be applied, thus providing for unobservability, a stronger property than either of the two along. On the other hand, consider another hypothetical system in which mixing networks are used to reach a third party broker requiring sign-in and authorization. Depending on the attacker type, this could mean that the mixing network unlinkability was cancelled out by the linkability due to entrusting the third party with identifying information in order to be authorized.

[7.](#) Privacy Evaluation

Now we turn our attention to the evaluation of privacy mechanisms in a standard form, given the attacker models and system definitions, for some of the example mechanisms.

An evaluation takes multiple parameters as input. The output of the evaluation template is based on the analysis of the individual algorithms, settings, and parameters passed to this evaluation mechanism.

Here is the top level interface of the evaluation template:

```
Eval(Privacy_Mechanism(param_1, param_2, ...),  
System_Setting(param_1, param_2, ...), Attacker_Model(param_1,  
param_2,...))
```

The output of the function is a privacy guarantee for the given settings, expressed through defined properties such as unlinkability and unobservability, for the specified system and attacker model.

7.1 Dummy Traffic Example

```
Eval(Dummy_Traffic (k=10, distribution=uniform), System_Setting([S,  
P, R, A], [S-P, P-R, R-A]), Attacker_Model(Type-1A, S-R)).
```

The dummy traffic mechanism is not presented as a practical mechanism, though there's no way to know if there are deployments of this type of mechanism. This example evaluation uses $k=10$ to indicate that for every one query initiated by an individual, ten queries that disguise the query of interest are selected uniformly at random from a pool of queries. In the parameters passed in the evaluation function, we indicate that the privacy assurances of

interest concern the S-R link, with a Passive Pervasive Monitor (Type-1A) attacker.

Here is a template format for the example:

Mohaisen & Mankin	Expires September 10, 2015	[Page 18]
-------------------	----------------------------	-----------

Internet-Draft	Evaluation of Privacy for DNS	March 2015
----------------	-------------------------------	------------

```
Eval(Dummy_Traffic (k=10, distribution=uniform),
    System_Setting([S, P, R, A],
        [S-P, P-R, R-A]),
    Attacker_Model(Type-1A, S-R)). {
    Privacy_Mechanism{
        Mechanism_name = Dummy_Traffic
        Parameters{
            Queries = 10
            Query_distribution = uniform
        }
    }
    System_settings{
        Entities = S, P, R and A;
        Links = S-P, P-R, R-A
    }
    Attacker_Model{
        Type = Type-1A
        Compromised_Entities = NA
        Links = S-R
    }
    Privacy_guarantee = undetectability
    Privacy_measure = 1-(1/(queries+1)).

    Return Privacy_guarantee, Privacy_measure
}
```

Undetectability is provided with .91 probability (though we know there are other weaknesses for dummy traffic) If the attacker model is replaced with Type-2, so that responses to arbitrary requests can be injected, and tracked, the undetectability probability is decreased.

7.2 Mixing Network Example

Here is an input for a mixing network privacy mechanism:

```
Eval(mix (u=10, distribution=uniform), System_Setting(link=S-R),
Attacker_Model(Type-1A)).
```

This indicates that the attacker resides between the stub and resolver. While queries are not undetectable, two queries are not linkable to the same individual; the provided guarantee is unlinkability. For a given number of individuals in the mixing network, indicated by the parameter u , assuming that at any time, traffic from these individuals is uniformly random, the probability that one query is comes from a given individual is $(1/10=0.1)$. The probability that two queries are issued by the same initiator is $0.1^2 = 0.01$, which represents the linkability probability. The

unlinkability probability is given as $1-0.01 = 0.99$. Thus,

```
(unlinkability, 0.99) < Eval(mix (u=10, distribution=uniform),
System_Setting(link=S-R), Attacker_Model(type-1A)).
```

We note that even if there is a Type-2 Attacker in R, the same results hold.

To sum up, the above example is represented in the following template:

```
Eval(mix (u=10, distribution=uniform),
  System_Setting([S, P, R, A],
    [S-P, P-R, R-A]),
  Attacker_Model(Type-1A, S-R)). {

  Privacy_Mechanism{
    Mechanism_name = mix    //mixing network
    Parameters{
```

```

        Users = 10
        Query_distribution = uniform
    }
    System_settings{
        Entities = S, P, R and A;
        Links = S-P, P-R, R-A
    }
    Attacker_Model{
        Type = Type-1A
        Entities = NA
        Links = P-R
    }

    Privacy_guarantee = unlinkability
    Privacy_measure = 1-(1/users)^2.

    Return privacy_guarantee, privacy_measure
}

```

7.3 Encrypted Channel (DNS-over-TLS) Example

For one of the encryption-based mechanisms, DNS-over-TLS [[dns-over-tls](#)], we have the following template (TLS parameters are from [[RFC5246](#)]):

Mohaisen & Mankin	Expires September 10, 2015	[Page 20]
-------------------	----------------------------	-----------

Internet-Draft	Evaluation of Privacy for DNS	March 2015
----------------	-------------------------------	------------

```

Eval(TLS_enc (SHA256, ECDSA, port 53, uniform, NA),
    System_Setting([S, P, R, A],
        [S-P, P-R, RA]),
        Attacker_Model(Type-1B, S-R)). {

    Privacy_Mechanism{
        Mechanism_name = TLS-upgrade-based
        Parameters{
            Users = NA
            Query_distribution = uniform
            Hash_algorithm = SHA256
            Sig_Algorithm = ECDSA
        }
    }
}

```

```

        Port 53
    }
    System_settings{
        Entities = S, P, R and A;
        Links = S-P, P-R, R-A
    }
    Attacker_Model{
        Type = Type-1B
        Entities = NA
        Links = S-R
    }

    Privacy_guarantee = unlinkability, undetectability
    Privacy_measure (unlinkability) = 1
    Privacy_measure (undetectability) = 0 // port 53 indicates DNS used

    Return privacy_guarantee, privacy_measure
}

```

This template features a Directed Monitor attack model (Type-1B) in order to show how that the monitor might apply extra resources to an encrypted channel. Undetectability is an issue whether using upgrade-based TLS on port 53, or a port-based TLS on a dedicated port – both ports indicate the use of DNS. The source address of the individual is exposed in all cases. If this were a suitably parameterized use of [[ipseca](#)], the attacker would not be certain that all the traffic from S-R was DNS, and undetectability would be higher.

7.4 Encrypted Channel (IPSec) Example

Template TODO

7.5 QName Minimization Example (R-A) Example

Template TODO

7.6 Encrypted Channel (S-R), QName Minimization (R-A) Example

Template TODO

7.7 Private-DNS (S-R) Example

The template for [[privatedns](#)] takes note of deployments in which in addition to S, R and A, there is another entity in the system, the function that authenticates the individual using S prior to permitting an encrypted channel to be formed to R or A. If the Private-DNS connection is with R, then identifiability of S as an individual may be similar to the identifiability of S from source address, or it may be stronger, depending on the nature of the account information required. If the Private-DNS connection is with A, source address PII is provided to A, and linkability of the queries from S has probability 1.

Template TODO

8. Security Considerations

The purpose of this document is to provide methods for those deploying or using DNS private exchange to assess the effectiveness of privacy mechanisms in depriving attackers of access to private information. Protecting privacy is one of the dimensions of an overall security strategy.

It is possible for privacy-enhancing mechanisms to be deployed in ways that are vulnerable to security risks, with the result of not achieving security gains. For the purposes of privacy evaluation, it is important for the person making an evaluation to also ensure close attention to the content of the Security Considerations section of each mechanism being evaluated, for instance, to ensure if TLS is used for encryption of a link against surveillance, that TLS best security practices [[uta-tls-bcp](#)] are in use.

[9.](#) IANA Considerations

No requests are made to IANA.

[10.](#) Acknowledgements

We thank Scott Hollenbeck, Burt Kaliski, Paul Livesay and Eric Osterweil for reviewing early versions. We also wish to thank those who commented on presentations of this work ahead of publication, including Simson Garfinkel, Cathy Meadows, Paul Syverson, and Christine Task.

11. Informative References

- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", [BCP 72](#), [RFC 3552](#), July 2003.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", [RFC 4949](#), August 2007.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", [RFC 6973](#), July 2013.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), May 2014.
- [RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", [RFC 7435](#), December 2014.
- [confidential-dns] Wijngaards, W. and G. Wiley, "Confidential DNS", [draft-wijngaards-dnsop-confidentialdns-03](#) (work in progress).

[dns-over-tls]

Zhu, L., Hu, Z., Heidemann, J., Wessels, D., Mankin, A., and P. Hoffman, "TLS for DNS: Initiation and Performance Considerations",
[draft-hzhwm-dprive-start-tls-for-dns-01.txt](#) (work in progress).

[dprive-problem]

Bortzmeyer, S., "DNS privacy considerations",
[draft-ietf-dprive-problem-statement-01](#) (work in progress).

[ipseca]

Osterweil, E., Wiley, G., Mitchell, D., and A. Newton, "Opportunistic Encryption with DANE Semantics and IPsec: IPSECA".

[openresolverproject.org]

Mauch, J., "The Open Resolver Project".

[phb-dnse]

Hallam-Baker, P., "DNS Privacy and Censorship: Use Cases

and Requirements", [draft-hallambaker-dnse-02](#) (work in progress).

[privatedns]

Hallam-Baker, P., "Private-DNS",
[draft-hallambaker-wsconnect-08](#) (work in progress).

[qname-minimisation]

Bortzmeyer, S., "DNS query name minimisation to improve privacy", [draft-ietf-dnsop-qname-minimisation-02](#) (work in progress).

[uta-tls-bcp]

Sheffer, Y., Holz, R., and P. StAndre, "Recommendations for Secure Use of TLS and DTLS", [draft-ietf-uta-tls-bcp-11](#) (work in progress).

Authors' Addresses

Aziz Mohaisen
Verisign Labs
12061 Bluemont Way
Reston, VA 20190
US

Phone: +1 703 948-3200
Email: amohaisen@verisign.com

Allison Mankin
Verisign Labs

12061 Bluemont Way
Reston, VA 20190
US

Phone: +1 703 948-3200
Email: amankin@verisign.com