

Evaluation of Privacy for DNS Private Exchange

<https://tools.ietf.org/html/draft-am-dprive-eval-02>

Allison Mankin
(with Aziz Mohaisen)
DPRIVE - IETF 94

A touch of Eval

- Draft is posted, feedback is very welcome!
 - draft-am-dprive-eval-02.txt
 - Many thanks to Tim Wicinski for his detailed feedback on the draft, including a DNS implementer approach to DNS evaluation.
- Current main structure
 - Same as in _01
 - See next

Keys

- Entities:
 - Attackers, eavesdropper, enabler, individual, initiator, intermediary, observer.
- Data analysis
 - Identifiability, personal names, and pseudonymity
 - Other notions from RFC4949; anonymity, sets, attributes, provider, relying party, etc.
- Other central notions
 - PII, subject, pseudonym, unlinkability, undetectability, and unobservability
- System model
 - DNS resolvers: S, R, A, and P
 - Setup: S-R, S-P, P-R, R-A
 - Main targeted link is S-R
- Risk model (monitors)
 - Type-1: passive pervasive
 - Type-2: active
 - In the system
- Mechanisms
 - Mix, dummy traffic, PIR, qname minimization, encryption and composed.

And evaluation templates!

Main Differences

- Consistent use of terms with other RFCs
 - Monitors instead of actors
 - Threat instead of risk
 - Mix networks instead of (both) mix and mixing
 - DNS exchange instead of communication.
- Major rewording through the draft to clear any ambiguity for evaluators.
- Recently published RFCs are referenced with their permanent numbers.

Main Differences

- The active monitor model is enriched
- Evaluation templates are reduced
 - Not provided parameters are removed (was NA)
 - Consistent presentation of interfaces
 - Consolidated multiple parameters without naming them into a set (params).

Question to WG

- Will the WG adopt this draft?
- Can it be submitted to fulfill the charter's evaluation deliverable?

Thank you!

Questions?