Privacy Enhancements for PowerDNS and DNSdist

NGI Trust and Privacy Enhancing Technologies Program

Alexander ter Haar
December 2020
<table>
<thead>
<tr>
<th>PowerDNS Recursor</th>
<th>PowerDNS Authoritative Server</th>
<th>PowerDNS DNSdist</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DNS resolving and caching server.</td>
<td>• Authoritative domain name hosting.</td>
<td>• Load Balancing,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DoH and DoT encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DDoS protection</td>
</tr>
</tbody>
</table>
Encryption of DNS Traffic

DNS Encryption is gaining traction

- DNS is one of the last remaining ‘non-encrypted’ protocols
- Risk interception of very personal data

Current Trend:

- DNS gets encrypted for a more secure connection from client to the resolver
- Client support for encrypted DNS is increasing
- IETF Encryption standard for DNS
  - DNS over TLS (DoT)
  - DNS over HTTPS (DoH)
DNS Privacy, Encryption, and DNS Providers

DNS Encryption with DoH and DoT

However:

- Interest is Encrypted DNS is increasing, but there is only limited uptake of encrypted DNS Services by network operators
- Browser Manufacturers are pushing for enhanced privacy to use this by default
- Number of ‘DoH’ providers is small, leading to centralization of DNS

There is a need for additional privacy friendly, European, DoH deployments to prevent DNS centralization.
Privacy Enhancements for PowerDNS and DNSdist

Goal:

• Enhance the availability of open, trustworthy, privacy respecting DNS software
  • Allows any DNS provider, operator, or others to provide encrypted and privacy-oriented DNS services.

• This project aims to improve or add additional privacy features to the open source PowerDNS software
PowerDNS and DNSdist
Privacy Enhancements
PowerDNS and DNSdist

Privacy Enhancements

- Encrypt Traffic between Recursor and Authoritative servers
  - Initial IETF proposal for ‘Discovery’
  - Implement (PoC/draft) discovery standards
PowerDNS and DNSdist

Privacy Enhancements

Encrypt Traffic between
Recursor and Authoritative servers
- Initial IETF proposal for 'Discovery'
- Implement (PoC/draft) discovery standards

DNSdist / DoH
- Deployment impr. (a.o. support http-caches)

DoH performance testing tool
PowerDNS and DNSdist

Privacy Enhancements

Encrypt Traffic between
Recursor and Authoritative servers
- Initial IETF proposal for ‘Discovery’
- Implement (PoC/draft) discovery standards

PowerDNS Recursor(s)

DNSdist

Qname minimisation
- Resolve step-by-step
- Improved heuristics

EDNS(0)padding
- Prevent information leakage

DNSdist / DoH
- Deployment impr. (a.o. support http-caches)

DoH performance testing tool

Internet
Summary

Privacy Enhancements for PowerDNS and DNSdist

• Encryption in DNS is gaining traction
  • Increased support on clients for DoH
  • a small number of parties offer encrypted DNS, bypassing traditional network resolvers
  • (so: This means more encrypted DNS traffic goes to less parties)

• To increase Privacy:
  • Privacy-focused (open source) DNS implementations and deployments is key
  • Allows EU operators (and others) to provide privacy-centric DNS

• This project implements further privacy enhancements for PowerDNS and DNSdist