DNS server privacy policy with assertion token

draft-reddy-dprive-dprive-privacy-policy-01

IETF 106, Singapore

Nov 2019

Presenter: T. Reddy (McAfee)

D.Wing (Citrix)

M. Richardson (Sandelman Software Works)

Agenda

- Problem statement
- Solution overview
- Privacy assertion token (PAT)
- PAT object

Problem statement: Users Need

1. **Find** DNS server privacy policy
2. Notice privacy policy **changes**
3. Policy **attestation**
4. Determine DNS filtering

Solution overview (1/4)

- **Finds** human readable DNS server privacy policy, **User does not have to search to find the privacy policy of the DNS server**

- **Machine-parsable DNS server privacy policy, that allows using a DNS server that complies with the DNS client's privacy policy.**
  - **Aligns with the proposed DROP structure in** https://tools.ietf.org/html/draft-ietf-dprive-bcp-op-05

- **Minimal human intervention to select a DNS server.**

Solution overview (2/4)

- Notice privacy policy **changes**
- **User is notified if the privacy policy claims of the DNS server have changed.**
- **Select a server that meets the privacy preserving data policy requirements of the client**

Solution Overview (3/4)

- policy **attestation**
  - signature by domain operating DNS server
  - optionally signed by third-party (“auditor”)
  - OV/EV certificates for privacy claims from registered organizations

Solution Overview (4/4)

- Determine DNS filtering
  - Malware Blocking
  - Policy Blocking

Privacy Information Claim

- It contains the privacy policy information of the server, it includes the following attributes:
  - IP address is PII or not
  - Logging of transaction data and duration.
  - User identity is logged and duration
  - DNS based content Filtering
    - Malware blocking
    - Policy Blocking
  - Transaction data shared with partners, names of partners and anonymized data shared with partners
  - Transfer data to third parties
  - Logging to notify user and Logging for analytics
  - Qname minimization
  - Privacy URL
  - Audit URL
  - Upstream server privacy claim and if the connection is secure.

Privacy assertion token (PAT)

- **PAT uses JSON Web Token (JWT) and JSON Web Signature (JWS)**
- **Client retrieves PAT per draft-ietf-dnsop-resolver-information.**
- **PAT object is created by the domain hosting the DoT/DoH server, and optionally by a third party privacy and security auditor of the DoT/DoH server.**

PAT object example

```
{
    "server":{
        "adn":["example.com"]
    },
    "iat":1443208345,
    "exp":1443640345,
    "privinfo": {
       "ipaddresspii":true,
       "logging": 24,
       "useridentity": 24,
       "sharedata": {
           "sharepartners": false
       },
       "transferdata":false,
       "privacyurl": "https://example.com/privacy/",
       "auditurl": "https://audit-example.com/privacyaudit"
    }
  }
```

PAT object example

```
JWS protected header:
{
     "alg":"ES256",
     "typ":"pat",
     "x5u":"https://cert.example.com/pat.cer"
}

JWS JSON:
{
  "payload":
"eyJhdWRpdHVyzOi8vYXVkaXQtZXhhbXBsZS5jb20vcHJpdmFjeWF",
  "signatures":[
       {"protected":"eyJhNiIsInR5cCI6InBhdCIsIng1dSI6Imh0dHB",
        "signature":
         "VeX23b4UNTRE358VKA1In-Nz5lpGVFXIjArnUY7T",
       {"protected":"eyJhbGciOiJdCIsIng1dSI6Imh0dHB",
        "signature":
         "PKLgWCegAT_TUo6fshOuuGrPqBSYRgIb2ApfvCENzdp-f"}]
}
```

draft-reddy-dprive-dprive-privacy-policy-01

- Comments and suggestions are welcome