draft-fieau-https-delivery-delegation-01

Frédéric Fieau - Orange
Iuniana Oprescu – Orange
Sergey Slovetskiy

IETF 94 - Yokohama

Latest changes

- Merged the two drafts related to the HTTPS delegation in CDNI context
  - draft-fieau-https-delivery-delegation (Fieau, Oprescu),
  - draft-slovetskiy-cdni-https-delegation-approaches (Slovetskiy)
- Clarified the HTTPS and DNS delegation issues and requirements
- Added a section on Third-party API for delegation (Keyless SSL)

Requirements for HTTPS delegation in CDNI

- Ensure the legitimacy of delegation
  - a uCDN has willfully designated the dCDN to deliver the requested content; the delegation is trusted.
- Ensure a “seamless” security redirection scheme
  - when redirecting user agents from one CDN to another: e.g. no security warning on user’ side
- Guarantee the confidentiality of CDNs configuration and topology information.

  e.g. need to “hide” CDNs hierarchy

HTTPS redirection

- Requirements check
  - Legitimate delegation is ensured
    - The uCDN sends back the dCDN URL to the user agent through the established secure HTTPS connection
  - Seamless security scheme is not (always) ensured
    - When the uCDN certificate is not valid for dCDN domain, the user-agent may display a warning
  - Confidentiality
    - e.g. CDNs hierarchy can be visible to the end-user
- Should be valid for all HTTPS redirection methods
  - 3xx directives
  - URL rewriting
  - API or scripted redirection

DNS redirection

- Requirements check
  - Legitimate delegation is not ensured
    - No guarantee that the uCDN has willfully designated the dCDN: a malicious DNS resolver could return DNS responses to steer the UA to a malicious server (HARD problem)
  - Seamless security scheme is not ensured
    - UA expects the uCDN certificate, but receives the dCDN certificate, a warning message is issued.
  - Confidentiality
    - CDNs hierarchy is not visible to the end-user, due to DNS protocol de facto
- Secured DNS-based delegation should be based on the use of DNSSEC.

Third-party API for delegation

- Guarantee a seamless security scheme for HTTPS redirection and trusted delegation

- Introduction of a Private Key Server in the TLS handshake.
  - The private keys remain under the authority of the content owner (e.g. the uCDN) while the content can be served from a dCDN
  - Split the setup of the secure connection between the client's browser and the surrogate delivering the content.
  - Such an architecture is commercially deployed (e.g. Keyless SSL)

- How:
  - When establishing TLS connection with the user agent, the dCDN will forward the challenge to the Private Key Server which is under the control of the content owner (or the uCDN).
  - The dCDN surrogate is then able to establish a secure connection to the end user without triggering any warnings in the client's browser.

Next steps

- Describe more clearly the Third-party API use case
- Detail token based solutions (URI signing)
- Add a section on XMPP POSH?