CDNI URI Signing

(draft-leung-cdni-uri-signing-01)

CDNI Working Group
IETF 85 Atlanta, Georgia
November 8, 2012

Kent Leung (kleung@cisco.com)
Francois Le Faucheur (flefauch@cisco.com)
Matt Caulfield(mcaulfie@cisco.com)

Background

URI Signing provides content access authorization:

- URI is embedded with information that can be validated to ensure the request has legitimate access to the content; symmetric or asymmetric keys used
- A signed URI is provided by the CSP (i.e. URI signer) to the user out of band (e.g. web site navigation)
- When the user selects the URI, the HTTP request is sent to the CDN.
- CDN validates the signed URI before delivering the content.
- BUT … there are no standards today

Multi-CDN Environment

URI Signing in CDNI:

- Downstream CDN advertises URI Signing capability
- When the user selects the URI (i.e. signed URI from CSP), the HTTP request is sent to the Upstream CDN which assigns the Downstream CDN
- HTTP request is sent to the Downstream CDN, which obtains the CDNI metadata (which includes URI Signing information) and validates the signed URI before delivering the content

Goal

- Standardize an extensible URI Signing method for base function with:
  - defined URI query string attributes
  - enhanced CDNI Interfaces
  - uCDN and dCDN operations
- HTTP-based request routing
  - Hop by hop, URI re-signed
- DNS-based request routing
  - Signed URI (to uCDN) is received by dCDN

  Note: DNS-based request routing using symmetric key is problematic when Delivering CDN does not have trust relationship with the CSP.

Base Information Set

Downstream CDN MUST have the following information:

- Part of the request that need to be validated (e.g. URI, IP header) [IP packet]
  - Resource and source IP address are protected by message digest
- Expiration of signed URI [URI query string]
  - Attribute in query string, protected by message digest
- Algorithm used for URI validation [metadata]
  - Entire URI or URI without scheme protected by message digest
- Hash function to apply to HMAC [metadata]
  - SHA1 or SHA256 as the base hash function?
- Access to key used for validation [metadata]
  - Key or reference to key such as URI
- Indication to enforce URI validation for content delivery [metadata]
  - Enforce indication set => signed URI is validated; plain URI is rejected
  - Enforce indication unset => signed URI is not validated; plain URI is allowed

"[]" denotes from where the information is obtained

Information Conveyed by URI

- URI Syntax (RFC 3986)

```
foo://example.com:8042/over/there?name=ferret#nose
\_/   \______________/\_________/ \_________/ \__/
 |           |            |            |        |
scheme   authority       path        query   fragment
```

- Two parts in the query component of URI:
  A. Attributes that convey authorization restrictions (e.g. source IP address and time period)
  B. Message digest that confirms the integrity and authenticity of the URI provided by the URI creator.

Information Conveyed by CDNI Interfaces

CFI

- URI Signing base support

CMI

- Algorithm used for URI validation
- Hash function to apply to HMAC
- Access to key used for validation
- Indication to enforce URI validation for content delivery

CLI

- No change

Issues Tracking

- Describe the general information needed for uCDN and dCDN
- Clean up the attributes needed for the URI query string
- Identify the CDNI metadata needed for URI Signing
- Clarify dCDN operation for combination of URI Signing enforcement indication and URI with and without URI signature
- Cover hop by hop HTTP request routing scenario
- Specify MUST/SHOULD/MAY in text
- Change details into pseudo code and move to later sections; ensure the URI signing and validation steps are used as reference for operational logic and not specific implementation sequence
- Flexible URI signing work item
- Identify CDNI footprint & capabilities advertisement parameters