Lightweight Authenticated Time (LATe) Synchronization Protocol

draft-navas-ace-secure-time-synchronization-00

Renzo Navas, Göran Selander, Ludwig Seitz

IETF 97, ACE WG. Seoul, Nov 17, 2016
Background/Motivation

- Freshness of information exchange can be assured by:
  - Time-stamps
  - Nonce-based exchanges

- Time-based solutions:
  - Typically have one less message than a nonce-counterpart protocol. Simplify exchanges/protocol: Good!
  - Drawback: There is the need for a (secure!) time synchronization protocol!

- ACE WG
    (except for an Introspection setting)
Background/Motivation

● A secure time-source is assumed on most security services (not only constrained). But, it does not yet exist…

  ○ NTPv4 authenticated mode incurs in a circular interdependence:
    ■ “The lifetime of cryptographic values must be enforced, which requires a reliable system clock. However, the sources that synchronize the system clock must be trusted.”
  ○ This problem is spotted and being solved at NTP WG “Network Time Security (NTS)” [I-D.ietf-ntp-network-time-security], it adds messages on top of a time protocol.

● … and these future solutions are not resource-constrained friendly.
Protocol Goals

- **Functional Goal:**
  - The protocol enables a constrained node to obtain a local time representation from a trusted entity, with an associated +/- uncertainty.

- **Security Goals:**
  - **Authentication:** The time representation must be authenticated (data authentication).
  - **Freshness:** The time representation must be fresh (RFC4949: “Recently generated; not replayed from some earlier interaction of the protocol.”)

- **Design Goals:**
  - Lightweight: Fewest messages possible, CBOR, COSE.
  - Easily transported over-foo, CoAP explicitly.
  - “ACE-embeddable”.

- **Non-goals:** accurate time precision
Proposed Solution: Base Protocol

\[ \text{Time} = \text{Time}_{TS} + \left( \frac{\text{RTT}}{2} \right) \]

Authentication(Nonce\_TC,TS\_Time)
Proposed Solution: TIC and TOC CBOR MAPs

### CBOR Map 'TIC Information'

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>CBOR Key</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonce</td>
<td>4 (TBD)</td>
<td>bstr</td>
<td>A random nonce</td>
</tr>
<tr>
<td>kid</td>
<td>5 (TBD)</td>
<td>bstr</td>
<td>Key-ID is an opaque value and identifies the cryptographic key to be used in the response</td>
</tr>
<tr>
<td>alg (optional)</td>
<td>6 (TBD)</td>
<td>int</td>
<td>Identifies the cryptographic algorithm to be used in the resp.</td>
</tr>
<tr>
<td>server (optional)</td>
<td>7 (TBD)</td>
<td>tstr</td>
<td>Identifies the intended Server for time synchr.</td>
</tr>
</tbody>
</table>

### CBOR Map 'TOC Response'

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>CBOR Key</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>3 (TBD)</td>
<td>uint (TBD)</td>
<td>A time representation information</td>
</tr>
<tr>
<td>nonce</td>
<td>4 (TBD)</td>
<td>bstr</td>
<td>A random nonce</td>
</tr>
</tbody>
</table>
## Proposed Solution: TIC and TOC CBOR MAPs

### CBOR Map 'TIC Information'

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>CBOR Key</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonce</td>
<td>4 (TBD)</td>
<td>bstr</td>
<td>A random nonce</td>
</tr>
<tr>
<td>kid</td>
<td>5 (TBD)</td>
<td>bstr</td>
<td>Key-ID is an opaque value and identifies the cryptographic key to be used in the response</td>
</tr>
<tr>
<td>alg (optional)</td>
<td>6 (TBD)</td>
<td>int</td>
<td>COSE Alg. Values</td>
</tr>
<tr>
<td>server (optional)</td>
<td>7 (TBD)</td>
<td>tstr</td>
<td>Identifies the intended Server for time synchr.</td>
</tr>
</tbody>
</table>

### CBOR Map 'TOC Response'

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>CBOR Key</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>3 (TBD)</td>
<td>uint</td>
<td>A time representation information</td>
</tr>
<tr>
<td>nonce</td>
<td>4 (TBD)</td>
<td>bstr</td>
<td>A random nonce</td>
</tr>
</tbody>
</table>

CBOR Map 'TOC Response', will be achieved by COSE.

Authentication of the CBOR 'TOC Response', will be achieved by COSE.
Example: TIC over CoAP

Time Server

/time

Time Client

(MSG1)

Header: POST (Code=0.02)
Uri-Host: "server.org"
Uri-Path: "time"
Content-Format: "application/late+cbor; late-type=tic"
Payload:

```json
{
    nonce : h'73616e206c6f7265',
    kid : h'0001',
    alg : 4 /* HMAC w/ SHA-256 truncated to 64 bits */
}
```

(CBOR Diagnostic notation)
Example: TOC over CoAP

Time Server

/time

Time Client

(MSG2)

Header: Changed (Code=2.04)
Content-Type: "application/late+cose;
cose-type=cose-mac; late-type=toct"

Payload:
{
  protected :
    {kid: h'0001',
     alg: 4 /* HMAC w/ SHA-256 truncated to 64 bits */},
  payload :
    {time : 14773107841,
     nonce : h'73616e206c6f7265'},
  tag    : h'36f5afaf0bab5d43'
}

(COSE-MACed 'TOC Response' in CBOR diagnostic notation)
LATe on ACE

● Actor Mappings:
  ○ Authorization Server (AS) is the Time Server
  ○ Resource Server (RS) is the Time Client
  ○ Client (C) will relay messages

● Possible Scenarios:
  ○ 1. First Message C -> RS: Resource Request
    ■ 1.1. Response: Time Synchronization only needed
    ■ 1.2. Response: Time Synchronization + Access Token needed
  ○ 2. First Message C -> AS: ACE Basic Protocol Flow
  ○ 3. First Message RS -> AS: Direct Communication (RS Can do Introspection)
LATe on ACE: Scenario 1.2.

AS (Time Server)  

C  


+-4.01 Unauthorized---+ 2. (ACE Info + TIC)

3. +---Token Request---+  
     + TIC

4. +---Token Response---+  
     + AUTH TOC

RS (Time Client)  

+-POST /authz-inf--->+ 5. (Token + AUTH TOC)

+-2.04 Changed------+ 6.
LATe on ACE: Scenario 1.2.
MSG 2: ACE Info + TIC

This response is not yet defined on ACE.
draft-gerdes-ace-dtls-authorize-00 defines “AS Information payload”
LATe on ACE: Scenario 1.2.
MSG 5: POST /authz-inf (Token+ Auth TOC)

C

5. /authz-inf

RS (Time Client)

Header: POST (Code=0.02)
Uri-Path:"authz-info"
Content-Format: "application/cwt+late; late-type=toe"
Payload:
{
toc : <COSE-MACed TOC Response>
cwt : <COSE-Encrypted CBOR Web Token>
}
Next Steps

- Cryptographically analyze/validate base protocol
  - Attacks were studied on paper. Test on a crypto model.
  - Involve a crypto person.

- Refine ACE Scenarios

- Get feedback from ACE WG
Discussion

Do we need a secure lightweight time synchronization mechanism?
Thank you!

Comments/Questions?
Backup Slides
LATe on ACE: Scenario 1.1