LwM2M need to maintain observation across security contexts. If DTLS session between LwM2M client and server changes for any reason, existing observations on the device could be maintained instead of requiring to re-send all the observations to the client. The reason behind this is also how LwM2M correlates the authorization of the client with the DTLS session and requires the client to re-register if the DTLS session changes, causing all observations to be re-sent.

The CoAP “Same Epoch” Requirement

Klaus Hartke

Joint IETF / OMA call
2019-02-26

RFC 7252:

> The following rules are added for matching a response to a request: The DTLS session MUST be the same, and the epoch MUST be the same.

RFC 7641:

> All notifications resulting from a GET request with an Observe Option MUST be returned within the same epoch of the same connection as the request.

Why? → Different epochs have different security properties.

Attack:

1. A client connects to a server using DTLS. The server authenticates with a server certificate; the client is unauthenticated.
2. The client sends a request that requires the client to be authenticated.
3. The server requests the client to authenticate.
4. The client authenticates with a client certificate; a new epoch starts.
5. The server processes the request, thinking it comes from the now authenticated client. Oops!

Requiring that the request is sent in the same epoch as the response prevents this attack. However, the requirement is quite broad and may prevent interesting use cases that do not have the same problem. The requirement could be narrowed down if a careful security analysis is made.

Possible solutions:

- Perform a careful security analysis under which circumstances it is safe to send a response in a different epoch and/or connection than the request.

- Use connection ID. Since no reconnection is needed when the IP address/port changes, the epoch stays the same.

- Configure the server with a configured request. https://tools.ietf.org/html/draft-bormann-core-responses-00#section-3