Constrained RESTful Environments WG (core)

Chairs:

Andrew McGregor <andrewmcgr@gmail.com>

Carsten Bormann <cabo@tzi.org>

Mailing List:

core@ietf.org

Jabber:

core@jabber.ietf.org

http://6lowapp.net

- **We assume people have read the drafts**

- **Meetings serve to advance difficult issues by making good use of face-to-face communications**

- **Note Well: Be aware of the IPR principles, according to RFC 3979 and its updates**

- Blue sheets
- Scribe(s): http://tools.ietf.org/wg/core/minutes

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session
The IESG, or any member thereof on behalf of the IESG
Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
Any IETF working group or portion thereof
Any Birds of a Feather (BOF) session
The IAB or any member thereof on behalf of the IAB
The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda Bashing

All times are in time-warped ART

Tuesday

- 17:40–17:50 Intro, WG status
- 17:50–18:15 CoAP over reliable WG draft (HT)
- 18:15–18:35 Resource Directory WG draft (MK)
- 18:35–18:50 Object Security 1 (GS)
- 18:50–19:10 SenML (AK)

All times are in time-warped ART

Friday

- **10:00–10:05 Intro, 🍺**
- **10:05–10:20 HTTP Mapping WG Draft (TF)**
- **10:20–10:35 Core Interfaces WG Draft (MK)**
- **10:35–11:20 COMI (PV)**
- **11:20–12:00 Object Security 2 (GS)**

6 years of CoRE WG

- 2009-07-28 “The 6LowApp Bar-BOF”
- 2010-03-09 CoRE WG chartered
  - Chairs: Cullen Jennings, Carsten Bormann
- 2012-02-14 Publication request (RFC 6690, Link-Format)
- 2012-09-10 New chair: Andrew McGregor
- 2013-03-13 Publication request (RFC 7252, CoAP)
- 2014-07-21 Publication request (RFC 7390, Groupcomm)
- 2014-07-20 Publication request (RFC 7641, Observe)
- 2015-09-14 Publication request (Block)
- 2016-04-04 Rechartered

Area Director: Handoff of the Baton

- **Lisa Dusseault** (chartered us)
- **Peter Saint-Andre** (from 2010)
- **Barry Leiba** (from 2012)
- **Alexey Melnikov** (from 2016)

WG documents

- draft-ietf-core-block — submitted to IESG
  - on IESG Telechat Agenda for 2016-04-21
- draft-ietf-core-http-mapping
  - WGLC completed → Friday
- draft-ietf-core-links-json
  - Discuss in context of RD below
- draft-ietf-core-resource-directory
  - → Today
- draft-ietf-core-interfaces
  - → Friday

CoAP over foo

- **draft-kivinen-802-15-ie**
- **draft-bormann-6lo-coap-802-15-ie**

All times are in time-warped ART

Tuesday

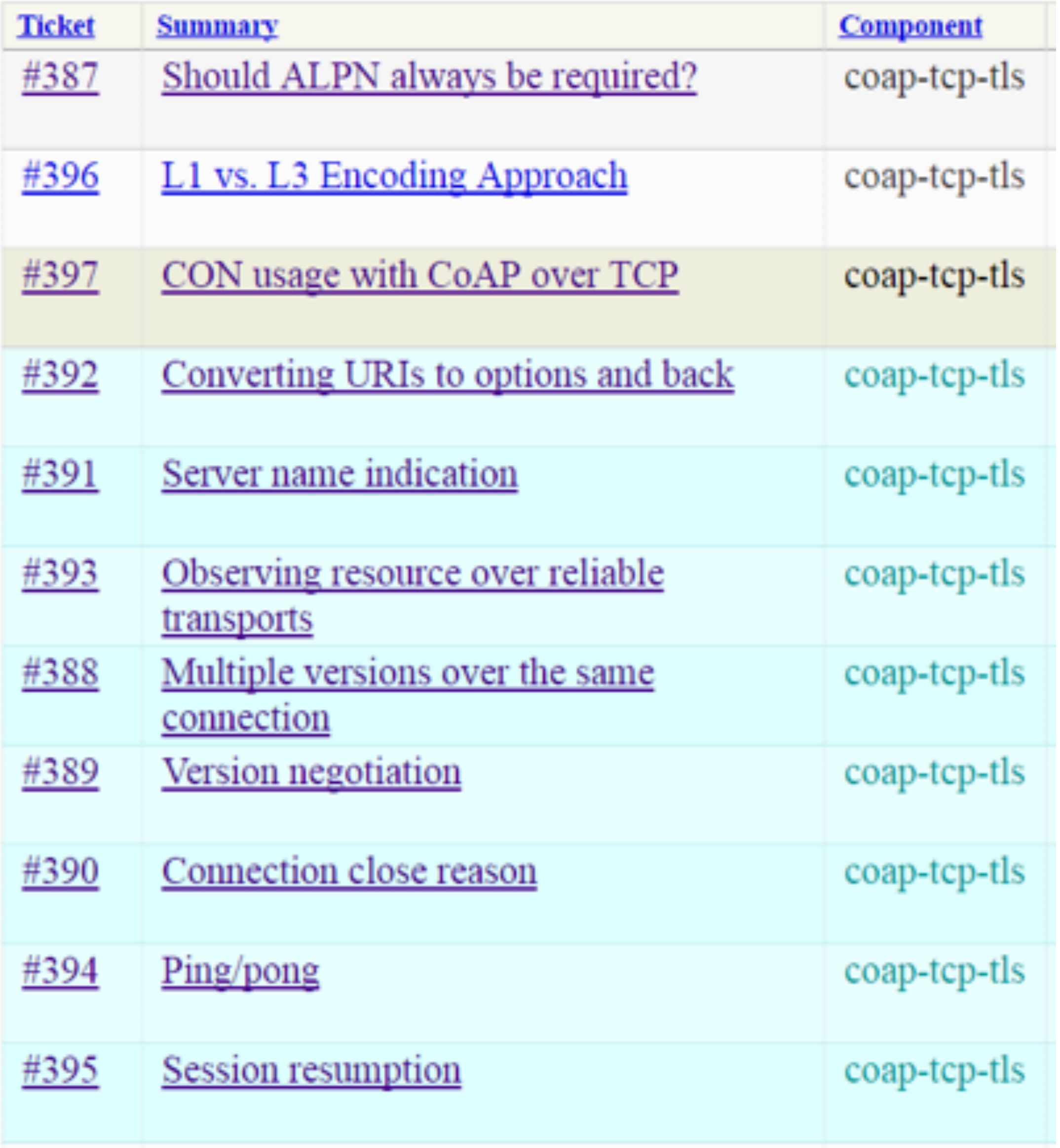
- **17:40–17:50 Intro, WG status**
- **17:50–18:15 CoAP over reliable WG draft (HT)**
- **18:15–18:35 Resource Directory WG draft (MK)**
- **18:35–18:50 Object Security 1 (GS)**
- **18:50–19:10 SenML (AK)**

CoAP over TCP

Hannes Tschofenig, Carsten Bormann, Simon Lemay

Open Issues at

https://trac.tools.ietf.org/wg/core/trac/report/1



Ticket	Summary	Component
#387	Should ALPN always be required?	coap-tcp-tls
#396	L1 vs. L3 Encoding Approach	coap-tcp-tls
#397	CON usage with CoAP over TCP	coap-tcp-tls
#392	Converting URIs to options and back	coap-tcp-tls
#391	Server name indication	coap-tcp-tls
#393	Observing resource over reliable transports	coap-tcp-tls
#388	Multiple versions over the same connection	coap-tcp-tls
#389	Version negotiation	coap-tcp-tls
#390	Connection close reason	coap-tcp-tls
#394	Ping/pong	coap-tcp-tls
#395	Session resumption	coap-tcp-tls

Issue #396: L1 vs. L3 approach

- Input from OIC on their use of CoAP
- In draft-tschofenig-core-coap-tcp-tls-04 we had 3 alternative encoding types:
  - L1: 16 bit length field
  - L2: 8/16/32 bit length field (CoAP / Major type 0 encoding)
  - L3: 8/16/32 bit length field (CoAP option encoding)
- If payload is larger than 64Kb → CoAP Block-wise Transfer needed. Block's largest block size is 1 KiB.
- Should we re-consider our solution approach?

Shim Header itself is insufficient

- Shim header with size information does not provide the capability to
  - Convey error messages (#390)
  - Exchange keepalive messages (#394)
  - Negotiation CoAP versions (#389)
  - Indicate the name of the server (#391)
- Should we design protocol functionality into the CoAP over TCP document?
  - More details at http://www.ietf.org/mail-archive/web/core/current/msg06979.html and http://www.ietf.org/mail-archive/web/core/current/msg06982.html.
- Alternative: Only allow TLS since it already provides the necessary functionality.

Size matters

- RFC 7252: stay around 1152 bytes max
- L1: 64 KiB max, L3: 4 GiB max
- Block: 1024 bytes max
    - (L1:) So when you go beyond 64 KiB, you suddenly need to go to 1 KiB blocks?

BERT: block-wise extension for reliable transport

- BERT defined for reliable (TCP/TLS/WS) only
- Use the remaining code point (SZX=7)
- But don't assign a specific size (e.g., 2048)
- Just use the payload provided
  - Doesn't work with reordering
  - There is no reordering with reliable!

So what about WebSockets?

- CoAP over WebSockets is of interest today to use CoAP in a Browser
  - Strictly speaking, this is a local interface
  - But it still helps to reuse components
- Draft is mature and has text we can use
- Proposal: Merge; move WebSockets to an appendix of the TCP/TLS document

Signaling Messages

- Signaling Protocol will expand until it is more complex than CoAP
- Don’t invent a new message format — we have a nice one
- Use 7.xx messages for signaling
  - Capabilities/Setting
  - Ping, Pong
  - Release, Abort

If needed

All times are in time-warped ART

Tuesday

- 17:40–17:50 Intro, WG status
- 17:50–18:15 CoAP over reliable WG draft (HT)
- 18:15–18:35 Resource Directory WG draft (MK)
- 18:35–18:50 Object Security 1 (GS)
- 18:50–19:10 SenML (AK)

CoRE Resource Directory

draft-ietf-core-resource-directory-07

Overview

- CoRE Resource Directory enables RESTful registration and discovery of network resources exposed by devices and services
- CoRE RD is used by OMA LWM2M in the Registration Interface
- RD is being integrated into new SDO work along with CoAP, for example OCF, W3C

Updates

- Use cases for resource catalogs and multiple ecosystem support (thread, OCF) may require alternate serializations of RFC6690
- Added content format (ct) to the hyperlink example in RD discovery
- Require support for application/link-format (40), make JSON and CBOR variants optional
- Some editorial corrections

Pending updates

- Recent implementation work generated some new issues, mostly clarifications
- Define what is required in implementation
- Keep service discovery in one place separate from resource discovery, sec. 5; finding an RD is not in the function set
- Don't refer to function sets, describe as REST API for registration, etc. more like hypermedia controls
- Remove redundant flow diagrams, use request and response descriptions
- Clarify how rd-group registration works vs. rd
- Clarify how rd-lookup constructs href of returned links
- Clarify how rd-lookup works with multiple lookup parameters
- Clarify what is required wrt. DNS compatibility
- Some editorial corrections, content format example

Roadmap

- Make pending corrections and update draft again for review – end of April
- Collect issues on CoRE Issue Tracker
- Late binding decision to include PATCH
- Schedule for WGLC?

CoRE working group

Fetch and Patch methods for CoAP

draft-vanderstok-core-etch-00

P. van der Stok, C. Bormann

Objective:

Payload Reduction

By transporting part(s) of a resource

Complex http URI’s

to focus on your interests

https://maps.google.com/maps?f=d&source=s_d&saddr=Millbrae+Caltrain+Station&daddr=&hl=en&geocode=&mra=ls&dirflg=r&ttype=dep&noexp=0&noal=0&sort=&sll=37.510543,-122.259507&sspn=0.012357,0.015235&ie=UTF8&lci=transit&start=0&ll=37.603641,-122.386107&spn=0.013566,0.018046&z=16&iwloc=lyrftr:m,0x808f77b091ff6be5:0x725e536abba2f0c6,37.599829,-122.386537

What if,
interest spec > ~ 1KiB?

- Switch to POST
    - can send detailed parameters in payload instead
- BUT,….. you loose GET properties (safe, idempotent)
- HTTP Search
    - Like GET
    - Add a body

CoAP FETCH

- Similar to HTTP SEARCH
  - Add request payload to a GET
- Slightly different semantics:
  - cacheable
  - request payload has a media type
    - Can define application-specific formats
  - Addressing Collections: e.g., **`[* selector]`**

CoAP PATCH

- Similar to HTTP PATCH
- Notes about caching and response codes
- Idem-potent version called iPATCH

CoAP Methods

Code	Name	Code	Name	safe	idempotent
0.01	GET	0.05	FETCH	yes	yes
0.02	POST	0.06	PATCH	no	no
0.03	PUT	0.07	iPATCH	no	yes
0.04	DELETE			no	yes

Core-Links-JSON

- Pretty much stable.
- Currently RFC 6690 and RFC 7390
- Extend RFC 6690 with more flexibility?
- Move the RFC 7390 part into a separate document?

Advanced Resource Directory Features

Akbar Rahman

IETF-95 (Buenos Aires), April 2016

https://tools.ietf.org/html/draft-rahman-core-advanced-rd-features-02

Introduction

- The Resource Directory (RD) is a key element for successful deployments of constrained networks

- Similar to the HTTP web search engines (e.g. Google), the RD for CoAP should also support useful search query responses beyond a basic listing of relevant links

- This draft proposes several new features to be considered for the RD. The only goal of this draft is to trigger discussion in the CORE WG so that all relevant features for RD evolution are taken into account during RD protocol development

Proposed RD Additional Features (1/)

- Explicit HTTP interfaces
  - Though there is now partial support of HTTP in [I-D.ietf-core-resource-directory], the RD function is intimately tied to the CoRE Link Format [RFC6690] which does not have any explicit support of HTTP at all.
  - So the CoRE Link Format probably needs to be updated to support HTTP explicitly?
    - For example, how will this work with the existing HTTP Link Header?

Proposed RD Additional Features (2/)

- Mirror Server
  - The CoRE WG has previously discussed the concept of a mirror server in relation to supporting sleepy devices.
  - Specifically, [I-D.vial-core-mirror-server] recommends to create a new class of RDs which store the actual resource representations (as opposed to simply storing the URI) in a special type of RD called the Mirror Server.
  - Communicating devices can both lookup the resource, and then also fetch directly the resource representation, from the Mirror Server regardless of the state of the sleepy server.
  - Should we continue developing this functionality?

Proposed RD Additional Features (3/)

- Re-direction to another RD
  - A given RD may not have the URIs being queried for registered in its database. The given RD should have the capability to re-direct the querying client to another RD which may have the information of interest.
- URI Ranking
  - Current Internet search engines have extensive methods for ranking the URIs returned to a human initiated search query
  - For example, the concept of Search Engine Optimization (SEO) has spawned a large industry in the web world for specifically this purpose
  - The concept of URI ranking (to indicate the "value" of the URI) should also be supported by the RD

Proposed RD Additional Features (3/)

- Re-direction to another RD
  - A given RD may not have the URIs being queried for registered in its database. The given RD should have the capability to re-direct the querying client to another RD which may have the information of interest.
- URI Ranking
  - Current Internet search engines have extensive methods for ranking the URIs returned to a human initiated search query
  - For example, the concept of Search Engine Optimization (SEO) has spawned a large industry in the web world for specifically this purpose
  - The concept of URI ranking (to indicate the "value" of the URI) should also be supported by the RD

Proposed RD Additional Features (5/)

- Privacy Model
  - IoT devices may often contain sensitive information (e.g. health monitoring device) or affect human safety (e.g. traffic light controllers, elevator actuators).
  - When the resources of a device is registered with a given RD and domain, should anyone at all be able to easily discover the resources associated with the device? Does this cause privacy or security concerns in certain RD lookup scenarios? If not, how really useful is the RD?
  - Currently, [I-D.ietf-core-resource-directory] has a very brief mention that endpoint and clients should be authenticated and access controlled. However, a more complete privacy model should be developed to address this very important issue.

Next Steps

- The proposed set of feature extensions for the RD will improve the constrained environment search capability and make deployments more efficient
- These RD feature extensions should be individually considered during the RD protocol development
- Evolution and forward thinking is required for the CoRE RD, as constantly occurs in the current Internet for HTTP web search engines

All times are in time-warped ART

Tuesday

- 17:40–17:50 Intro, WG status
- 17:50–18:15 CoAP over reliable WG draft (HT)
- 18:15–18:35 Resource Directory WG draft (MK)
- 18:35–18:50 Object Security 1 (GS)
- 18:50–19:10 SenML (AK)

Requirements for CoAP End-To-End Security

draft-hartke-core-e2e-security-reqs-00

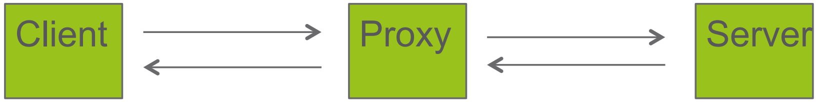
Göran Selander, Ericsson
Francesca Palombini, Ericsson
Klaus Hartke, Universität Bremen TZI
Ludwig Seitz, SICS Swedish ICT

IETF 95, CORE WG, Buenos Aires, Apr 5, 2016

Introduction

- CoAP uses DTLS for security
- CoAP relies on proxies for scalability and efficiency
- The proxy operations on CoAP messages requires DTLS to be terminated at the proxy
- Therefore the proxy has access to the data required for performing the proxy functionality
- The proxy also able to eavesdrop on or manipulate any part of the CoAP payload and metadata in transit between client and server or inject new CoAP messages
- This is neither protected nor detected by DTLS
- One way to mitigate this is to secure CoAP communication at the application layer using COSE
- Such a mechanism can provide "end-to-end security" at the application layer in contrast to the "hop-by-hop security" provided by DTLS

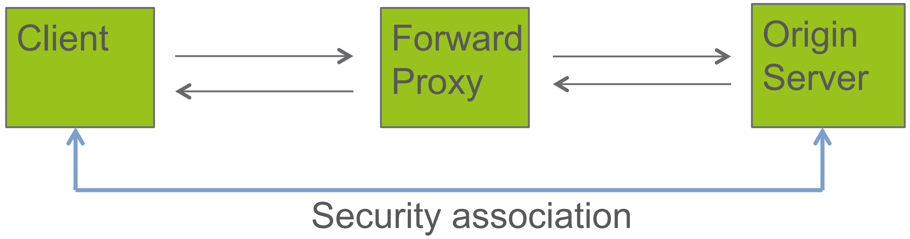
Scope and Assumption

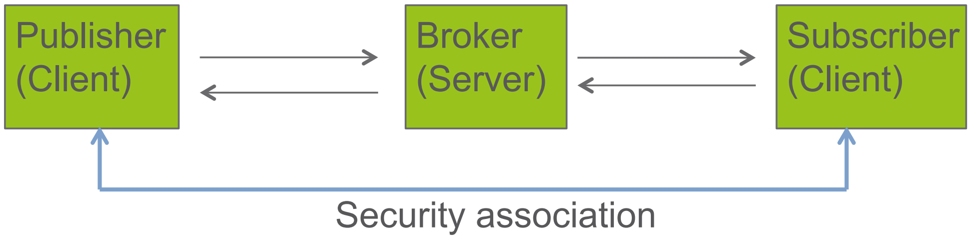


- The basic function of a proxy is to process a message according to certain processing rules. For example:
  - Forward a message to the next proxy when the link is up
  - Only forward a request if there is no fresh cached response
  - Forward a new publication to all subscribing clients

Scope and Assumption

- A security solution is needed that protects against certain threats while still allowing the proxy to assume its normal functionality
- The client and server are assumed to have a security association
- The proxy is neither assumed to have a security association with the client nor with the server





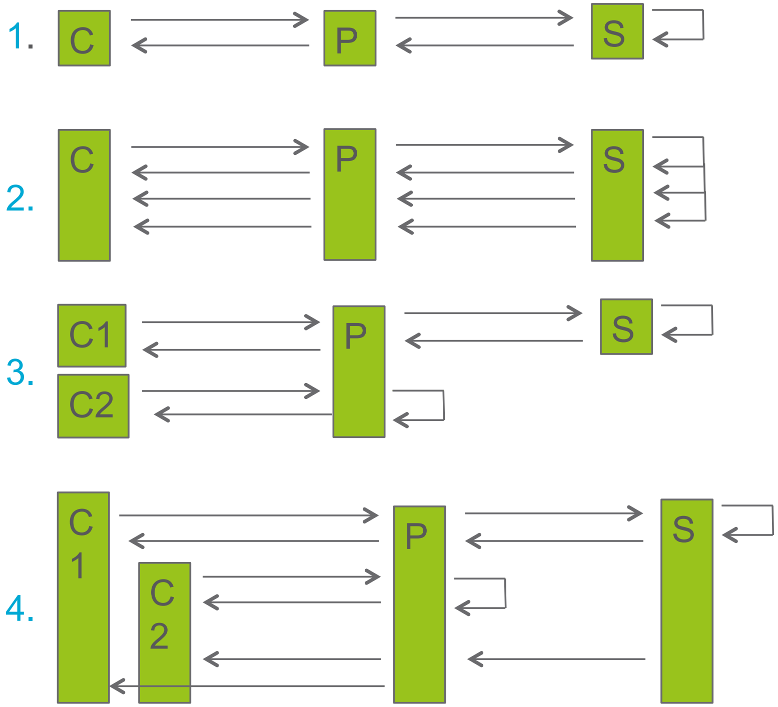
Methodology

1. Identifying assets associated to sensor- and actuator-based communication
2. Specifying the processing rules of intermediary nodes in different scenarios
3. Defining security objectives relevant for the scenarios
   - E.g. a caching proxy needs access to the cache key, which thus cannot be encrypted end-to-end
4. Considering the potential threats executed through proxies
5. Defining security requirements (and non-requirements) that an end-to-end security mechanism for CoAP needs to meet.

Scenarios Overview

1. One Request - One Response
   - Example: Alarm status retrieval
2. One Request - Multiple Responses
   - Example: Secure parameter monitoring
3. Multiple Requests - One Response
   - Example: Caching
4. Multiple Requests - Multiple Responses
   - Example: Observe with multiple observers
5. Multiple Requests - Multiple Responses
   - Example: Publish-Subscribe

Note that since CoAP was not designed for end-to-end security, some scenarios extend the applicability of CoAP beyond its original scope.



Discussion & Next Steps

- More work is needed to specify the precise processing operations for scenarios 3 - 5.
- We plan to add reverse proxy and cross-protocol proxy (such as HTTP-CoAP proxy) in the next version. Other important settings missing?

- Some of the scenarios have mutually exclusive security/functionality objectives (caching vs challenge-response) – more than one solution is required.
- Some of the scenarios have very similar requirements – not one solution per scenario.

- Follow the progress of the draft at: https://github.com/ektrah/coap-object-security

Thank you!

Comments/questions?

All times are in time-warped ART

Tuesday

- **17:40–17:50 Intro, WG status**
- **17:50–18:15 CoAP over reliable WG draft (HT)**
- **18:15–18:35 Resource Directory WG draft (MK)**
- **18:35–18:50 Object Security 1 (GS)**
- **18:50–19:10 SenML (AK)**

Media Types for Sensor Markup Language (SenML)

draft-jennings-core-senml-06

IETF 95, Buenos Aires, Argentina

Ari Keränen
ari.keranen@ericsson.com

Base values

- Old: can appear in any SenML Record and use merge-patch format to update previous
  - Compact with varying base values **but** requires to process SenML Records sequentially (“streaming”)

Base values

- New proposal: base values **only** in first Record
  - Multiple base values -> multiple SenML Packs
  - Base (if any) and data values mixed in 1st record
  - All base labels start with b (non-base SHALL NOT)
- Why not “Base Record” with only base values?
  - Often only single measurement -> empty base records
  - Variant type arrays problematic in some cases

Example

```
[
  { "bn": "urn:dev:ow:10e2073a01080063",
    "t": 1276020076, "v":23.5, "u":"Cel" },
  { "t": 1276020091, "v":23.6, "u":"Cel" }
]
```

Links

- For adding more metadata in-line and for future extensions
- To be defined by draft-ietf-core-links-json

```
[{ "bn": "http://[2001:db8::2]/",
   "bt": 1320078429,
   "bl": "[{\"href\":\"humidity\",\"foo\":\"bar1\"},
    {\"href\":\"temperature\",\"foo\":\"bar2\",
    \"bar\":\"foo3\"}]\" },
 { "n": "temperature", "v": 27.2, "u": "Cel" },
 { "n": "humidity", "v": 80, "u": "%RH" }
]
```

Privacy sensitive names

- Long-term stable unique identifiers are problematic for privacy reasons [RFC7721]

Other updates

- CDDL definitions
- Label registry (for extensions)
- Terminology (SenML Record & SenML Pack)
- Note about long-term stable IDs
- XML part needs still work for consistency

- We assume people have read the drafts
- Meetings serve to advance difficult issues by making good use of face-to-face communications
- Note Well: Be aware of the IPR principles, according to RFC 3979 and its updates

✓Blue sheets
✓Scribe(s)

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session
The IESG, or any member thereof on behalf of the IESG
Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
Any IETF working group or portion thereof
Any Birds of a Feather (BOF) session
The IAB or any member thereof on behalf of the IAB
The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

All times are in time-warped ART

Friday

- 10:00–10:05 Intro, 🍺
- 10:05–10:20 HTTP Mapping WG Draft (TF)
- 10:20–10:35 Core Interfaces WG Draft (MK)
- 10:35–11:20 COMI (PV)
- 11:20–12:00 Object Security 2 (GS)

Area Director: Handoff of the Baton

- **Lisa Dusseault**
  (chartered us)

- **Peter Saint-Andre**
  (from 2010)
- **Barry Leiba**
  (from 2012)

- **Alexey Melnikov**
  (from 2016)

All times are in time-warped ART

Tuesday

- **17:40–17:50 Intro, WG status**
- **17:50–18:15 CoAP over reliable WG draft (HT)**
- **18:15–18:35 Resource Directory WG draft (MK)**
- **18:35–18:50 Object Security 1 (GS)**
- **18:50–19:10 SenML (AK)**

All times are in time-warped ART

Friday

- 10:00–10:05 Intro, 🍺
- 10:05–10:20 HTTP Mapping WG Draft (TF)
- 10:20–10:35 Core Interfaces WG Draft (MK)
- 10:35–11:20 COMI (PV)
- 11:20–12:00 Object Security 2 (GS)

Guidelines for HTTP-CoAP Mapping Implementations

Angelo Castellani, Salvatore Loreto, Akbar Rahman, Thomas Fossati, Esko Dijk

IETF-95 (Buenos Aires), April 2016

https://tools.ietf.org/html/draft-ietf-core-http-mapping-09

Main Changes in rev-08 (1/2)

- Changes from rev-07 to rev-08:
  - Addressed WGLC comments from Klaus Hartke as outlined in:
    - https://www.ietf.org/mail-archive/web/core/current/msg06866.html
  - Summary of main updates in -08 to address Klaus' comments:
    - Updated the Use Cases (Section 4) to clarify that the HTTP client sending the HTTP Request may optionally insert a CoAP URI inside the HTTP URI
      - Only if a CoAP URI is inserted, the Section 5 for URI mapping applies
    - Updated Section 6.5 (Content Transcoding) for handling of diagnostics messages as per suggestion from Klaus

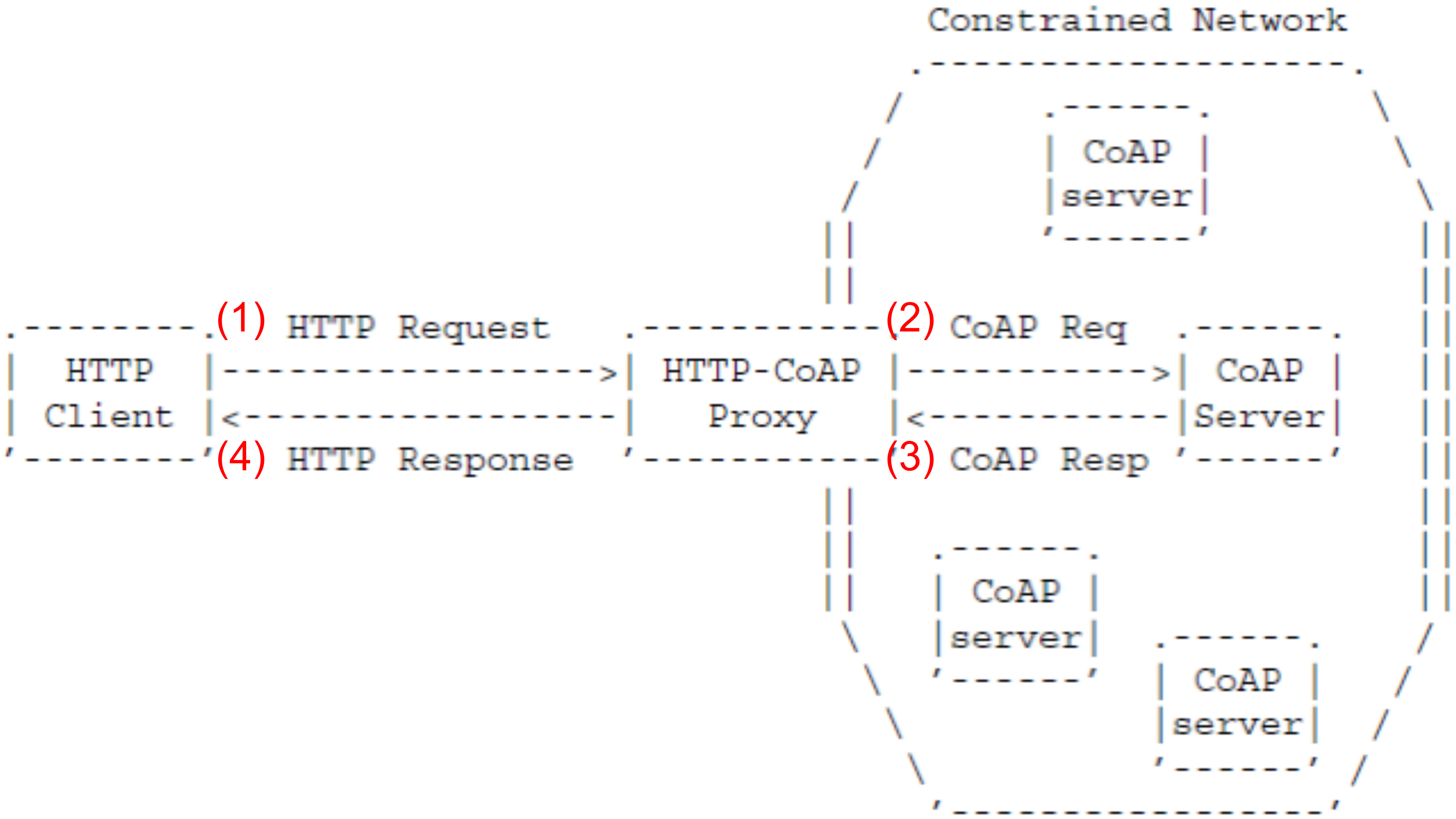
Main Changes in rev-08 (2/2)

- Changes from rev-07 to rev-08 (Continued):
    - Updated Section 7 (Response Code Mapping) as per several suggestions from Klaus
    - Updated Section 8.1 (Caching and Congestion Control) as per several suggestions from Klaus
- Klaus wrote back this Tuesday and indicated that he was satisfied with the answers to his original comments
    - (But with one new comment about clarifying between reverse and forward proxies → see proposed rev-10 changes slide):
    - https://www.ietf.org/mail-archive/web/core/current/msg07013.html

Main Changes in rev-09

- Scrubbed requirements keywords (SHOULD, MUST, etc.) to only apply to requirements introduced by this draft:
  - Removed requirements language for those taken from other RFCs and convert to lower case
  - Also, while we were doing the scrub we felt that there were a few cases of extraneous text which we just deleted as they were tending to over specify the Proxy operation.

Cross-Protocol Proxy Deployment Scenario



Proposed Changes for rev-10 (1/2)

- Clarify that scope of draft is primarily Reverse HC Proxy but that also covers generic protocol translation aspects that apply as well to Forward and Interception HC Proxy
  - e.g. Response status mapping & content format mapping apply to all types of proxies
- Clarify that draft concentrates on certain direction of the translation from HTTP to CoAP (i.e. the HC proxy is a HTTP server and a CoAP client)
- Clarify that CoAP RFC 7252 section 10.2 (HTTP-CoAP Proxying) is not enough to specify full proxy behavior because it basically covers mapping of Methods and simple response code mapping

Proposed Changes for rev-10 (2/2)

- Terminology cleanup:
  - Remove references to “placement” of proxy (e.g. server-side vs client-side) as is confusing and provides little added value

- Section 3 (Reverse HTTP-CoAP Proxy)
  - Remove the “reverse” from section and figure title
  - Add separate paragraphs for forward proxy and interception proxy

- Fix reference corruption that occurred in -09 due to outdated xml2rfc tool local cache

Next Steps

- Need to contact IANA to start discussions on:
  - New Resource Type of “rt=core.hc” (for discovering reverse HTTP-CoAP proxy function)
  - New “coap-payload” Internet Media Type
  - Do we need to register proposed new link format attribute of “hct” somewhere?
    - “…the new target attribute "hct" is defined in this document. This attribute MAY be returned in a "core.hc" link to provide the URI Mapping Template associated to the mapping resource.”
- Should we have another WGLC round?

All times are in time-warped ART

Friday

- **10:00–10:05 Intro, 🍺**
- **10:05–10:20 HTTP Mapping WG Draft (TF)**
- **10:20–10:35 Core Interfaces WG Draft (MK)**
- **10:35–11:20 COMI (PV)**
- **11:20–12:00 Object Security 2 (GS)**

All times are in time-warped ART

Friday

- 10:00–10:05 Intro, 🍺
- 10:05–10:20 HTTP Mapping WG Draft (TF)
- 10:20–10:35 Core Interfaces WG Draft (MK)
- 10:35–11:20 COMI (PV)
- 11:20–12:00 Object Security 2 (GS)

All times are in time-warped ART

Friday

- **10:00–10:05 Intro, 🍺**
- **10:05–10:20 HTTP Mapping WG Draft (TF)**
- **10:20–10:35 Core Interfaces WG Draft (MK)**
- **10:35–11:20 COMI (PV)**
- **11:20–12:00 Object Security 2 (GS)**

Object Security of CoAP (OSCOAP)

draft-selander-ace-object-security-04

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 95, CORE WG, Buenos Aires, Apr 8, 2016

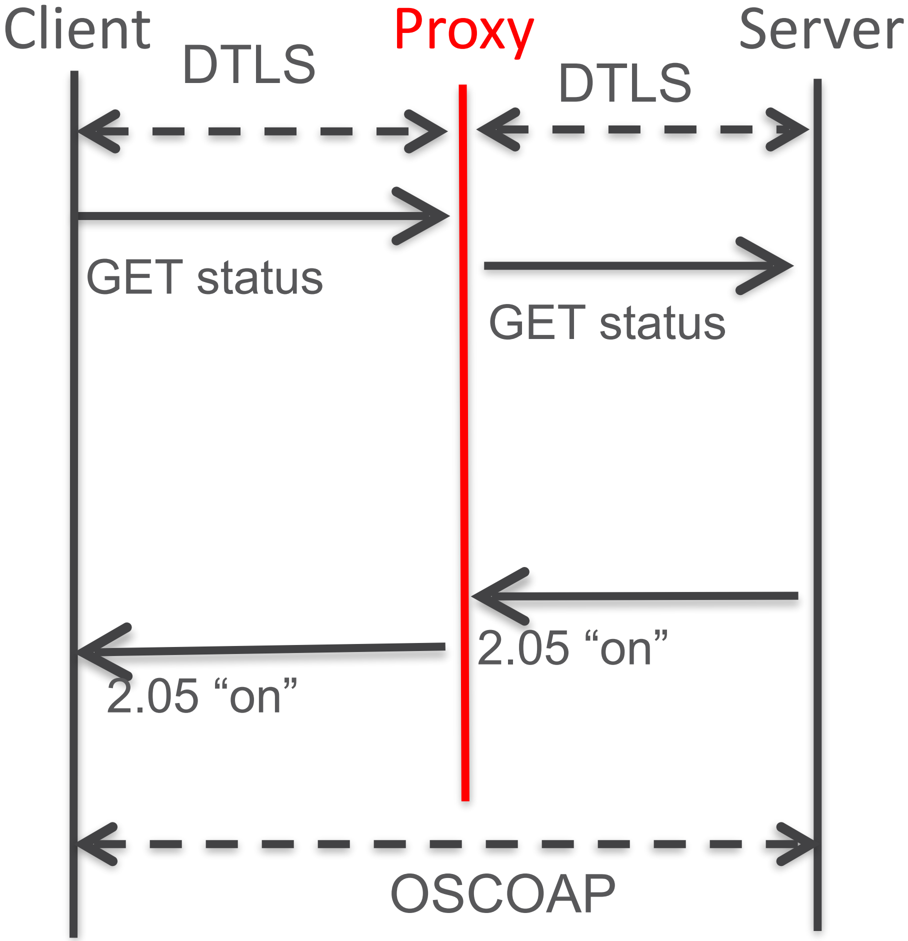
OSCOAP

- OSCOAP is a security protocol protecting CoAP messages using COSE objects and an “Object-Security” option

- Independent of how CoAP is transported (UDP, TCP, foo…)

- OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations

- Related draft: [draft-hartke-core-e2e-security-reqs]()



Re-structuring: more implementation details

Table of Contents

4 main parts:

- The CoAP Object-Security option
- The security context
- The COSE object
- The OSCOAP protocol

Appendixes:

- Size expansion
- Examples
- OSCON (Object Security of Content)

Alignment with existing work:

- Security Context - TLS 1.3 (use of AEAD ciphers, key derivation, nonce construction…)

  (draft-ietf-tls-tls13-12)

- Protected CoAP message data – COSE object

  (draft-ietf-cose-msg-11)

Message expansion using OSCOAP

- Updated examples and size calculation
- Compliant with COSE -11

Tid	Tag	COSE OH	Message OH
5 bytes	8 bytes	9 bytes	22 bytes

Figure 9: Message overhead for a 5-byte Tid and 8-byte Tag.

- From Appendix A.4

All options are encrypted…

…except those intended to be changed by forward proxy

No.	C	U	N	R	Name	Format	Length	E	I	D
1	x			x	If-Match	opaque	0-8	x	x	
3	x	x	-		Uri-Host	string	1-255			
4				x	ETag	opaque	1-8	x	x	
5	x				If-None-Match	empty	0	x	x	
6		x	-		Observe	uint	0-3	x	x	x
7	x	x	-		Uri-Port	uint	0-2			
8				x	Location-Path	string	0-255	x	x	
11	x	x	-	x	Uri-Path	string	0-255	x	x	
12					Content-Format	uint	0-2	x	x	
14		x	-		Max-Age	uint	0-4	x	x	x
15	x	x	-	x	Uri-Query	string	0-255	x	x	
17	x				Accept	uint	0-2	x	x	
20				x	Location-Query	string	0-255	x	x	
35	x	x	-		Proxy-Uri	string	1-1034			
39	x	x	-		Proxy-Scheme	string	1-255			
60			x		Size1	uint	0-4	x	x	

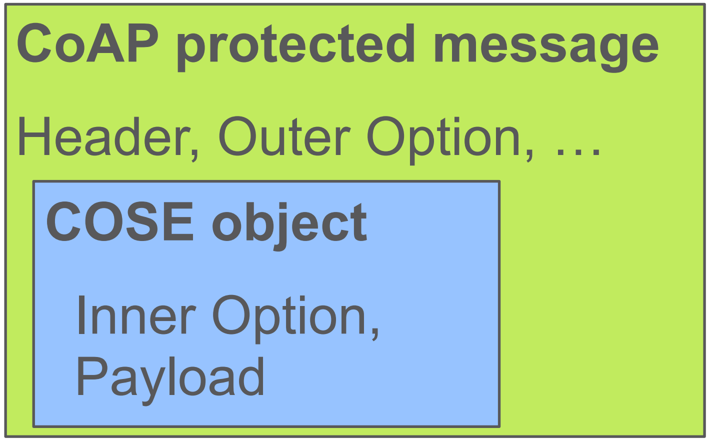
C=Critical, U=Unsafe, N=NoCacheKey, R=Repeatable,
E=Encrypt, I=Integrity Protect, D=Duplicate.

Figure 4: Protected CoAP Options

Duplicate options

- Encrypted options are carried in the COSE object
- We introduce **Duplicate of an option** which is in the Options part of the CoAP protected message.

- In version -04:
  - Max-age
  - Observe



CoAP protected message

Header, Outer Option, …

COSE object

Inner Option,
Payload

- One instance is sent encrypted (“Inner” option) the other in clear (“Outer” option)
  - “Inner” and “Outer” relative to the secure COSE object
- The Inner option value is intended for the end-point, the Outer option value is intended for the proxy

What’s next

- Include Blockwise (next slide)
- CoAP over TCP
- New implementations in progress
- Release as open source
- ACE profiles based on OSCOAP

Blockwise

Block* and Size* are Duplicate options

- The endpoint can fragment and protect each block with OSCOAP. The Block* option are encrypted (Inner Block* option)
- A proxy can fragment each protected OSCOAP message, thus adding an unprotected option (Outer Block* option)
- The “Inner” and “Outer” options are **independent**

- Adding a policy for maximum size of the inner fragments prevents an adversary from adding outer options and sending fragments ad infinitum.
- The inner blocks need to be cryptographically linked

Acknowledgement

- Much of the improvement in the content of this version is the result of the security analysis done in the requirements document, which is joint work with Klaus Hartke
- Klaus is already mentioned in the acknowledgements section but not in this respect
- We will remedy this in the next version

Thank you!

Comments/questions?