

T2TRG: Thing-to-Thing Research Group

Implementers' Workshop

October 27, 2016, Ludwigsburg (Stuttgart), Germany

Chairs: Carsten Bormann & Ari Keränen

Note Well

- You may be recorded
- The IPR guidelines of the IETF apply:
see **<http://irtf.org/ipr>** for details.

Administrivia (I)

- Pink Sheet
- Note-Takers
- Off-site (Jabber, Hangout?)
 - **<xmpp:t2trg@jabber.ietf.org?join>**
- Mailing List: **t2trg@irtf.org** — subscribe at:
<https://www.ietf.org/mailman/listinfo/t2trg>
- Repo: **<https://github.com/t2trg/2016-10-implementers>**

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (2)

Afternoon

- 13:45 (Matthias, all) API issues (CoAP, RD), memory management
- 14:05 (Carsten, all) alternative transports, NAT traversal, offline notification
- 14:35 (all) Dynamic addresses, CoAP endpoints, and DTLS
- 15:05 (Julien, all) Security on low-throughput networks
- 15:25 (Julien, all) Observing large resources; patch notifications
- 15:45 (Julien, all) Large implementation clustering issues
- 16:05 Coffee Break
- 16:30 (Carsten, all) Privacy-enhanced session resumption, long-term identifiers revisited
- 17:00 (all) emerging topics (e.g., more on DTLS)
- 18:00 (Chairs) Wrapup; next steps
- 18:30 End of meeting
- 19:00 Dinner

T2TRG scope & goals

- Open research issues in turning a true "Internet of Things" into reality
 - Internet where low-resource nodes ("things", "constrained nodes") can communicate among themselves and with the wider Internet
- Focus on issues with opportunities for IETF standardization
 - Start at the IP adaptation layer
 - End at the application layer with architectures and APIs for communicating and making data and management functions, including security

Done so far

- Chartered in December 2015. Multiple meetings before official chartering co-located with IETF meetings and with W3C Web of Things (WoT) group
- 2016: RG meetings at Nice and Lisbon co-located with W3C WoT, at San Jose co-located with IAB IoT**SI** WS, at Buenos Aires and Berlin with the IETF meetings; participated in Dublin IAB IoT**SU** WS; RIOT summit in Berlin
- Three RG deliverable documents in progress on REST and security; multiple new documents on REST interaction
- Outreach (e.g., organizations like OCF and Bluetooth SIG)

Where are we going

- Work on RG deliverables and outreach continues
- Future meetings co-located with good research venues (2017)
- Meetings co-located with open source activity
 - RIOT summit in Berlin (July)
 - Eclipse IoT meeting (here)
- Benchmark/reference scenarios
 - Initial discussion in various drafts and slides
 - More elaborate documentation by end of 2016

Next meetings

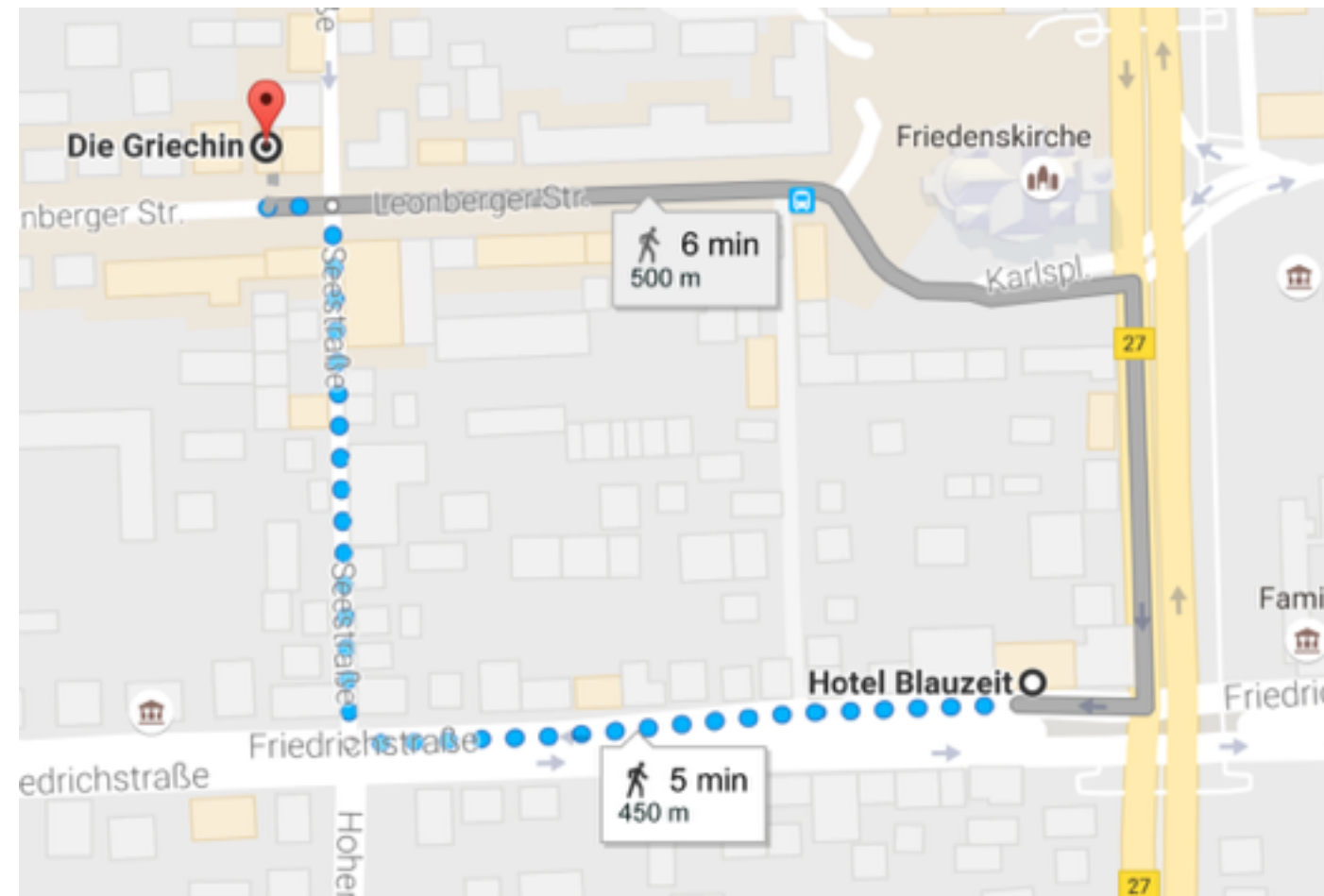
- Meet with ICNRG in Seoul before IETF97 (Sun Nov 13)
 - Issue worth discussing: data naming
- Academic: February @EWSN?
 - Maybe look at system issues (radio to application)

Lunch

- Approx. 12:30

Restaurant "Die Griechin"

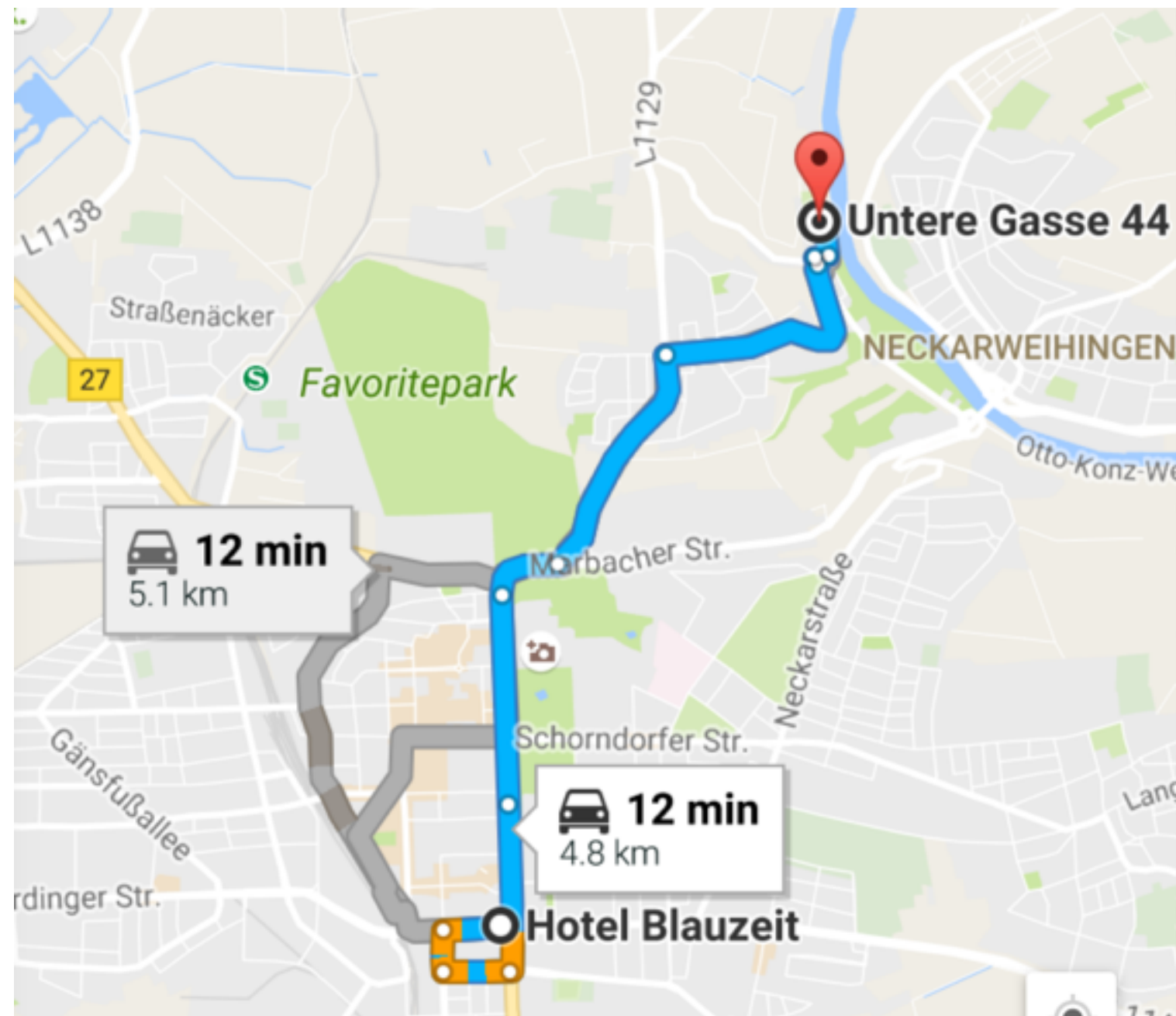
Leonberger Str. 23 / 1



<http://www.die-griechin.de/speisekarte/mittagstisch/index.html>

Dinner

- Table of 15± booked at 19:00 at Krone Alt-Hoheneck
- Car-pooling required



Thank you,

- Siemens, for the room,
- Ericsson, for the refreshments,
- Eclipse, for the organization

Agenda (1)

Morning

09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
09:30 Matthias Kovatsch Californium issues and statement of direction
10:00 Olaf Bergmann libcoap issues and statement of direction
10:20 Ziran Sun IoTivity issues and statement of direction
10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
10:55 (Chairs) other CoAP implementations
11:10 Coffee Break
11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
11:45 Olaf Bergmann tinydtls issues and statement of direction
12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
12:30 Lunch

Agenda (1)

Morning

09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing

09:30 Matthias Kovatsch Californium issues and statement of direction

10:00 Olaf Bergmann libcoap issues and statement of direction

10:20 Ziran Sun IoTivity issues and statement of direction

10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction

10:55 (Chairs) other CoAP implementations

11:10 Coffee Break

11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction

11:45 Olaf Bergmann tinydtls issues and statement of direction

12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling

12:30 Lunch

Agenda (1)

Morning

09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
09:30 Matthias Kovatsch Californium issues and statement of direction
10:00 Olaf Bergmann libcoap issues and statement of direction
10:20 Ziran Sun IoTivity issues and statement of direction
10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
10:55 (Chairs) other CoAP implementations
11:10 Coffee Break
11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
11:45 Olaf Bergmann tinydtls issues and statement of direction
12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
12:30 Lunch

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (1)

Morning

09:00	Chairs	Welcome, Meeting overview, T2TRG Status, Agenda Bashing
09:30	Matthias Kovatsch	Californium issues and statement of direction
10:00	Olaf Bergmann	libcoap issues and statement of direction
10:20	Ziran Sun	IoTivity issues and statement of direction
10:40	Tobias Rohde, Tobias Kaupat	Lobaro CoAP issues and statement of direction
10:55	(Chairs)	other CoAP implementations
11:10	Coffee Break	
11:30	Kai Udalla, Matthias Kovatsch	Scandium issues and statement of direction
11:45	Olaf Bergmann	tinydtls issues and statement of direction
12:00	(Chairs)	other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
12:30	Lunch	

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (1)

Morning

- 09:00 Chairs Welcome, Meeting overview, T2TRG Status, Agenda Bashing
- 09:30 Matthias Kovatsch Californium issues and statement of direction
- 10:00 Olaf Bergmann libcoap issues and statement of direction
- 10:20 Ziran Sun IoTivity issues and statement of direction
- 10:40 Tobias Rohde, Tobias Kaupat Lobar CoAP issues and statement of direction
- 10:55 (Chairs) other CoAP implementations
- 11:10 Coffee Break
- 11:30 Kai Udalla, Matthias Kovatsch Scandium issues and statement of direction
- 11:45 Olaf Bergmann tinydtls issues and statement of direction
- 12:00 (Chairs) other DTLS implementations; DTLS issues: CBC, DTLS 1.3, compatibility, stapling
- 12:30 Lunch

Agenda (2)

Afternoon

- 13:45 (Matthias, all) API issues (CoAP, RD), memory management
- 14:05 (Carsten, all) alternative transports, NAT traversal, offline notification
- 14:35 (all) Dynamic addresses, CoAP endpoints, and DTLS
- 15:05 (Julien, all) Security on low-throughput networks
- 15:25 (Julien, all) Observing large resources; patch notifications
- 15:45 (Julien, all) Large implementation clustering issues
- 16:05 Coffee Break
- 16:30 (Carsten, all) Privacy-enhanced session resumption, long-term identifiers revisited
- 17:00 (all) emerging topics (e.g., more on DTLS)
- 18:00 (Chairs) Wrapup; next steps
- 18:30 End of meeting

- 19:00 Dinner

Agenda (2)

Afternoon

13:45 (Matthias, all) API issues (CoAP, RD), memory management

14:05 (Carsten, all) alternative transports, NAT traversal, offline notification

14:35 (all) Dynamic addresses, CoAP endpoints, and DTLS

15:05 (Julien, all) Security on low-throughput networks

15:25 (Julien, all) Observing large resources; patch notifications

15:45 (Julien, all) Large implementation clustering issues

16:05 Coffee Break

16:30 (Carsten, all) Privacy-enhanced session resumption, long-term identifiers revisited

17:00 (all) emerging topics (e.g., more on DTLS)

18:00 (Chairs) Wrapup; next steps

18:30 End of meeting

19:00 Dinner

CoAP over TCP, TLS, ...

- <http://tools.ietf.org/html/draft-ietf-core-coap-tcp-tls-05.txt>
- In WG last-call (till 2016-11-01)
 - Just send your comments to core@ietf.org
- Covers TCP, TLS/TCP, Websockets (WS), WSS

Why TCP?

- Within Backend: More efficient for large amounts of messages
- For NAT traversal: TCP NAT bindings live much longer than UDP NAT bindings (device-to-cloud scenario)

Why Websockets?

- Browsers don't do CoAP natively yet
- Web application front-ends can speak CoAP over Websockets to a hub or a cloud endpoint
- (Also, Websockets are sometimes last resort for firewall traversal)

Framing

- TCP: Add length field to demarcate messages
 - After some waffling, adopted “L3” variant (as OCF)
 - Not needed for Websockets
- Leave out message-ids and message types
 - message reliability covered by TCP

BERT

- Block-wise not needed if a large message-size is agreed
- But can cause head-of-line blocking
- BERT: Just send multiple 1024-byte blocks in one CoAP message
- $SZX=7$

Signaling Messages

- Signaling Messages are about the connection, not about a request/response pair
- Standard CoAP message format, use 7.xx codes
- SM Option numbers are specific to a 7.xx code

CSM

- Capability and Settings Messages
- MUST be exchanged at the start (not in current OCF!)
- Capabilities: Block transfer, Message size > 1152
- Can do SNI

Ping/Pong

- A Ping elicits a Pong (echoing Token)
- Custody option in Pong:
“I really have processed everything up to the Ping”

Release, Abort

- Release: Orderly release
 - Hold-off option if this was for load-shedding
 - Can give Alternate-Address
- Abort:
At least give a reason before slamming the receiver
- Can use diagnostic payload in either (please do!)

Agenda (2)

Afternoon

13:45 (Matthias, all) API issues (CoAP, RD), memory management

14:05 (Carsten, all) alternative transports, NAT traversal, offline notification

14:35 (all) Dynamic addresses, CoAP endpoints, and DTLS

15:05 (Julien, all) Security on low-throughput networks

15:25 (Julien, all) Observing large resources; patch notifications

15:45 (Julien, all) Large implementation clustering issues

16:05 Coffee Break

16:30 (Carsten, all) Privacy-enhanced session resumption, long-term identifiers revisited

17:00 (all) emerging topics (e.g., more on DTLS)

18:00 (Chairs) Wrapup; next steps

18:30 End of meeting

19:00 Dinner

Endpoints

- Endpoint: you || the other party that you are talking to
- Initiator (Client):
Server learns about it when the request hits
- Responder (Server):
Client needs to “find” it (from URI data)

Endpoints in HTTP

- Server endpoint: Scheme/Host/Port (**Origin**)
 - Translated to Address/Port by client (**DNS**)
 - HTTPS: Client verifies DNS name of Host (**PKI**)
- Client endpoint: anonymous
 - Can use Client Address/Port (usually considered ephemeral)
 - Client certs: rare
 - Put Client identity into **Cookie** (muddled up with application state)

What's different in CoAP

- **DNS** deemphasized
- Certs (and thus **PKI**) deemphasized
 - PKI Certs need CRLs/OCSP, secure absolute time, ...
- We don't have **cookies**
- **Servients**: Servers often have client component
— how to link their identities?

Endpoints in CoAP/UDP

- Client uses **URI data** to look up server transport address
 - lookup mechanism intentionally not defined in RFC 7252
- Server uses **request transport address** to reply and send notifications

CoAP/UDP: Issues

- Endpoint transport addresses might not be stable
 - IP addresses change due to renumbering
 - Transport addresses change due to NAT timeouts
- Transport address change loses endpoint identity

CoAP/UDP: Issues

- Server address change:
 - New requests:
Lookup mechanism likely to use cache → stale info
 - Observe, other long-running requests:
Client cannot relate Notification to the right server
- Client address change:
 - Observe, other long-running requests:
Server cannot send Notification to the right client

Endpoints in CoAP/DTLS

- Client uses **URI data** to look up server transport address
- Client states (**SNI**) and verifies server identity (and server possibly verifies client identity)
- Endpoint is the peer in the resulting **connection**
 - Ephemeral: endpoint dies with connection
 - (but long-term endpoint “identity” doesn’t)

SNI: Server Name Indication

- SNI: TLS option for client hello
 - Tells Server what cert to send in the server hello
- In HTTPS, derived from DNS name (hostname)
 - Can't do that for IP address
- “Common” cop-out: Use RD EP id for SNI

“Identity”

- Most misunderstood word in security
- Identity = set of claims
 - But that’s not how we use the term intuitively
- Need another word for the “real-world identity” of a Thing
 - But what is that? Owner change, role change, repairs (replace board/chip)...
- Where authorization is entirely identity-based: need “revocation”

Endpoint claims in HTTPS

- server: DNS name
(tied into Authority and thus Origin)
 - Cert can actually have other claims,
but those are rarely visible to application
- client: (could have cert, but usually:)
established in-band, then reified into cookies

Endpoint claims in COAPS

- PSK mode: mutual verification
 - needs out of band channel; cf. DCAF
 - source, scope specified by those OOB mechanisms
- RPK mode: implicit server identity claim
 - OOB channel can be used (e.g., with directed identity)
- Cert mode: less well-defined (could use HTTPS model)

Implicit vs. Explicit Claims

- PSK: Implicit claim of existing security association
- RPK: Implicit claim of server possession of private key
 - Both can be augmented by OOB information
- Cert: Explicit claim of SNI possession (time-bounded)
- With CWT, have more fine-grained, explicit claims:
 - Issuer, Audience, Scope, ...

Identity confusion in APIs

- Very little of this makes it into APIs
- E.g., IoTivity uses the transport address as endpoint identity — even with DTLS
 - Application may send data via new, unrelated DTLS connection that happens to have the same transport address
- Issue: How to represent endpoints in APIs?

CoAP/DTLS: Issues

- DTLS connection tied to transport address pair
 - dies when either pair changes
- Current request/response matching includes “epoch”
 - does not even extend Observe across session resumption

Resumption

- Could extend matching (and thus endpoints) across resumption
- Issues:
 - garbage collection (when to discard session state?)
 - who is responsible for resumption?
 - (what exactly is the security semantics?)

Drafts to read

- draft-hummen-dtls-extended-session-resumption-01.txt (2013): **prepare** for resumption
- draft-barrett-mobile-dtls-01.txt (2009): send connection identifier to enable resumption later

Agenda (2)

Afternoon

- 13:45 (Matthias, all) API issues (CoAP, RD), memory management
- 14:05 (Carsten, all) alternative transports, NAT traversal, offline notification
- 14:35 (all) Dynamic addresses, CoAP endpoints, and DTLS
- 15:05 (Julien, all) Security on low-throughput networks
- 15:25 (Julien, all) Observing large resources; patch notifications
- 15:45 (Julien, all) Large implementation clustering issues
- 16:05 Coffee Break
- 16:30 (Carsten, all) Privacy-enhanced session resumption, long-term identifiers revisited
- 17:00 (all) emerging topics (e.g., more on DTLS)
- 18:00 (Chairs) Wrapup; next steps
- 18:30 End of meeting
- 19:00 Dinner