T2TRG: Thing-to-Thing proposed Research Group

Thing-to-Thing RG (T2TRG)
Buenos Aires, AR
Summary meeting 2016-04-07

Prof. Dr.-Ing. Carsten Bormann
TZI – Universität Bremen
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-ietf95
Agenda

- 16:20 Chairs  RG overview, status
- 16:30 Ari  RESTful design  draft-keranen-t2trg-rest-iot
- 16:35 Mohit  Secure bootstrapping survey  draft-sarikaya-t2trg-sbootstrapping
- 16:45 Chairs  Outreach, cooperation
- 16:51 Matthias  Interaction models, hypermedia controls
- 17:03 Chairs  Schema interoperability: call for contributions
- 17:15 Chairs  Meeting planning
Agenda

• 16:20 Chairs    RG overview, status
• 16:30 Ari       RESTful design    draft-keranen-t2trg-rest-iot
• 16:35 Mohit     Secure bootstrapping survey    draft-sarikaya-t2trg-sbootstrapping
• 16:45 Chairs    Outreach, cooperation
• 16:51 Matthias   Interaction models, hypermedia controls
• 17:03 Chairs    Schema interoperability: call for contributions
• 17:15 Chairs    Meeting planning
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

- Multiple meetings before official chartering; co-located with IETF meetings and with W3C
- 2016: RG meeting at Nice co-located with W3C, and at San Jose co-located with IAB IoTSI WS
- Three RG deliverable documents in progress on REST and security (present two today)
- Outreach (e.g. orgs 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
  • Planning to start with RIOT summit in July 2016
• Benchmark/reference scenarios
  • Initial discussion in various drafts and slides
  • More elaborate documentation by end of 2016
Agenda

• 16:20 Chairs  RG overview, status
• 16:30 Ari   RESTful design  draft-keranen-t2trg-rest-iot
• 16:35 Mohit Secure bootstrapping survey  draft-sarikaya-t2trg-sbootstrapping
• 16:45 Chairs  Outreach, cooperation
• 16:51 Matthias Interaction models, hypermedia controls
• 17:03 Chairs  Schema interoperability: call for contributions
• 17:15 Chairs  Meeting planning
RESTful Design for Internet of Things Systems

draft-keranen-t2trg-rest-iot-01
Ari Keränen <ari.keranen@ericsson.com>
with Matthias Kovatsch & Klaus Hartke

T2TRG @ IETF95
Goal of the Document

• “Guidance for designing IoT systems that follow the principles of the REST architectural style”
• Collect terminology
• Key information + pointers to details
• With IoT focus in examples etc.
• ... while keeping it quick and easy to read
Where we are now

-01 out
  - More terminology
  - Clarified idempotency and application state
  - What’s different with IoT (data formats, interaction patterns, etc.)

Remaining key topics including
  - Resource and media type design
  - Hypermedia-driven applications
  - Design patterns
Read/Comment/Spread the <3

• [draft-keranen-t2trg-rest-iot-01](draft-keranen-t2trg-rest-iot-01)
• Reviews and comments very welcome
• What would you like to see info about?
• Make other orgs aware of this
Agenda

- 16:20 Chairs  RG overview, status
- 16:30 Ari  RESTful design  draft-keranen-t2trg-rest-iot
- 16:35 Mohit  Secure bootstrapping survey  draft-sarikaya-t2trg-sbootstrapping
- 16:45 Chairs  Outreach, cooperation
- 16:51 Matthias  Interaction models, hypermedia controls
- 17:03 Chairs  Schema interoperability: call for contributions
- 17:15 Chairs  Meeting planning
Secure IoT Bootstrapping: A Survey

draft-sarikaya-t2trg-sbootstrapping-00

Behcet Sarikaya, Yizhou Li,
Mohit Sethi, Robert Cragie
Secure Bootstrapping

• What is bootstrapping and what is security bootstrapping?
  – Many definitions out there

• "it is the process by which a thing/device/smart object in an IoT network securely becomes operational at a given location and point of time."

• Possible goals of secure bootstrapping:
  – Identity: authentication of a pre-established identity vs. creation of a new identity
  – Authorization for network access, incl. configuration of communication parameters
  – Registration or joining a domain or group
  – Pairing with a specific node, or connecting to a cloud service

• This definition is broad on purpose since the term IoT itself represents a very diverse spectrum of applications
  – pairing of phones over bluetooth to exchange files, and
  – securely connecting IEEE 802.15.4 sensors factory to the backend both require some form of secure bootstrapping
Managed methods

• Pre-established trust relations and authentication credentials
• Centralized or federated
• Examples:
  – AAA / Extensible Authentication Protocol (EAP)
  – Generic Bootstrapping Architecture (GBA) with SIM
  – Open Mobile Alliance (OMA) Light-weight M2M:
    • Factory Bootstrap, Bootstrap from Smartcard, Client Initiated, Bootstrap
    • Server Initiated Bootstrap
  – Kerberos
  – Vendor certificates
P2P / ad-hoc methods

• No pre-established credentials
• Out-of-band channel used for distributing or confirming keys
  – Typically Diffie-Hellman exchange + MitM prevented with OOB communication
• Examples:
  – Bluetooth simple pairing
  – Wi-Fi protected setup
  – EAP-NOOB (out-of-band authentication for EAP)
  – Magic wand, e.g. commissioning tool in I-D.kumar-6lo-selective-bootstrap
Opportunistic / leap-of-faith methods

• Continuity of identity or connection, rather than initial authentication
• Some methods assume that the attacker is not present at the initial setup
• Examples:
  – SEND and CGA
  – WPS push button
  – SSH, gmail, Facebook
Hybrid methods

• Most deployed methods are hybrid:
  • Components from both managed and ad-hoc methods
  • E.g. central management after ad-hoc registration
• Categorization is not always easy or clear

• Choice of bootstrapping method depends heavily on the business case:
  – What third parties available?
  – Who wants to retain control or avoid work?
  – Manufacturer/vendor, system admin, user, fully ad-hoc
Secure Bootstrapping

• Why we need a survey:
  – Learn the design assumptions and trade-offs
  – NOT produce a 100 page document
  – Help developers choose what option is suitable.
  – End-of-life and re-bootstrapping are complex:
    https://www.iab.org/wp-content/IAB-uploads/2016/03/draft-farrell-iotsi-00.txt
Agenda

• 16:20 Chairs    RG overview, status
• 16:30 Ari       RESTful design    draft-keranen-t2trg-rest-iot
• 16:35 Mohit     Secure bootstrapping survey    draft-sarikaya-t2trg-sbootstrapping
• 16:45 Chairs    Outreach, cooperation
• 16:51 Matthias  Interaction models, hypermedia controls
• 17:03 Chairs    Schema interoperability: call for contributions
• 17:15 Chairs    Meeting planning
Outreach & Cooperation

• Objective: Mutual Education with IoT SDOs
• Make sure that
  • SDO people know how to interact with IETF
  • SDO people know about IETF products
  • v.v.
Outreach & Cooperation

- **Ongoing**: joint meetings with W3C IG Web of Things (WoT)
- **Once** (so far): Joint meeting with Open Connectivity Foundation (OCF); increasing involvement.
- **Starting**: First activities with Bluetooth SIG
- **Future**:
  - Other relevant orgs (which?)
  - Pull in relevant academia
  - Interact with open source activities
Agenda

- 16:20 Chairs  RG overview, status
- 16:30 Ari  RESTful design  draft-keranen-t2trg-rest-iot
- 16:35 Mohit  Secure bootstrapping survey  draft-sarikaya-t2trg-sbootstrapping
- 16:45 Chairs  Outreach, cooperation
- 16:51 Matthias  Interaction models, hypermedia controls
- 17:03 Chairs  Schema interoperability: call for contributions
- 17:15 Chairs  Meeting planning
Semantic Interoperability Requires Self-describing Interaction Models

IRTF T2TRG Activity Report, IETF 95, Buenos Aires, AR
Matthias Kovatsch (matthias.kovatsch@siemens.com)
Information Model for Interoperability

• Make use of data produced by IoT devices
• Well understood that data must be meaningful

➔ About the “what”

• Domain-specific requirements have led to multiple consortia
• Each consortium has defined their own data model
• Inferred meta model could help to bridge between data models
Interaction Model for Interoperability

• Machine-to-machine communication
• Make APIs machine-understandable

→ About the “how”

• Integration of descriptions on the server side is straight-forward
• Consumption on the client side is challenging
• Missing abstractions have led to hard-coded clients
Handling Change

- Add new things
- Also control future things
- Still control old things
- Control alternative things
Semantic Interoperability

• Information model
  • Describing the exchanged information ➔ vocabulary
  • Must allow for linking/bridging data models from different domains
  • W3C WoT: Semantic model such as RDF

• Interaction model
  • Describing the possible interactions ➔ vocabulary
  • Must allow for change and diversity
  • T2TRG: Hypermedia-driven applications (HATEOAS)
T2TRG: Interaction Model with Hypermedia Controls

- Hypermedia As The Engine Of Application State (HATEOAS)

- Composition of multiple resources models things
- Atomic interaction steps (request-response) shape processes
- Links and forms describe how requests must be formulated
- Relation vocabulary attaches meaning (shared a priori)
- Publication of links and forms allows for change (shared at runtime)
Idea

Client

Entry URI

Submit forms

Action Result

Follow links

Resource Directory

Thing A

Dynamically extend process flow

Auth-Server

Thing B

Choice & redundancy

Thing C

Thing D

Programming Abstractions?
CoRAL


The Web link (in RFC 5988 syntax):

```html
<coap://example.com:5683/info/tos>
;rel=terms-of-service;type=text/plain
```

is serialized in CoRAL as follows:

```json
[
  /abs_link/ 0,
  /terms-of-service/ 64,
  [
    /format/ 3, 0 /text/plain/,
    /href.scheme/ 4, "coap",
    /href.host.name/ 6, "example.com",
    /href.port/ 11, 5683,
    /href.path/ 12, "info",
    /href.path/ 12, "tos"
  ]
]
```
Summary

• Semantic Interoperability
  • Information model ↦ W3C WoT IG/WG
  • Interaction model → hypermedia-driven applications

• Scenarios
  • Reference scenario → requirements and challenges
  • PlugREST scenario → prototyping and interoperability testing

• Building Blocks
  • Machine-understandable links and forms
  • Representation formats (hypermedia) for IoT applications
  • Guidelines for programming abstractions
Agenda

- 16:20 Chairs  RG overview, status
- 16:30 Ari  RESTful design  
- 16:35 Mohit  Secure bootstrapping survey 
- 16:45 Chairs  Outreach, cooperation
- 16:51 Matthias  Interaction models, hypermedia controls
- 17:03 Chairs  Schema interoperability: call for contributions
- 17:15 Chairs  Meeting planning
Schema Interoperability

- Good discussions at the IAB IoTSI workshop and T2TRG meeting in March
  - »There will not be one schema, not even one schema language«
- Collect, integrate schemas/ontologies
- Translate between schema/modeling languages
What is that hub?
Data loss?
Translating data between data models vs. Translating data models
Data/Information Models vs. Interaction Models
How far can we get?

Limits to translation (e.g., security?)
Schema Interoperability

• What is the research that we should be encouraging?
Agenda

• 16:20 Chairs    RG overview, status
• 16:30 Ari       RESTful design    draft-keranen-t2trg-rest-iot
• 16:35 Mohit     Secure bootstrapping survey    draft-sarikaya-t2trg-sbootstrapping
• 16:45 Chairs    Outreach, cooperation
• 16:51 Matthias  Interaction models, hypermedia controls
• 17:03 Chairs    Schema interoperability: call for contributions
• 17:15 Chairs    Meeting planning
Meeting Planning

- IoT SDO Outreach: Keep up the pulse
- Open Source: Start with RIOT, what next?
- Academic Research venues: Start planning for 2017
Meeting Planning

• Pretty firm:
  • Track at RIOT Summit, Berlin 2016-07-15/-16 (Fri-Sat) (before Berlin IETF96)
  • ~Thu-Sun September 22-25 (with and after W3C at Lisbon)

• To do:
  • around IETF97 at Seoul? (November 14-18 2016)
  • Good research venue(s) (2017)
IoTSU

- Software Update of IoT devices
  - Not a research problem!
  - Or is it?
- June 13–14, Dublin? (Deadline May 22?)